(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/084456 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB02/01645

(22) International Filing Date: 11 April 2002 (11.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0109200.6	12 April 2001 (12.04.2001)	GB
0111528.6	11 May 2001 (11.05.2001)	GB
0126583.4	6 November 2001 (06.11.2001)	GB
0126929.9	9 November 2001 (09.11.2001)	GB

(71) Applicant *(for all designated States except US)*: **NET-DESIGNS LIMITED** [GB/GB]; Raines Business Centre, Raines House, Denby Dale Road, Wakefield, West Yorkshire WF1 1HR (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **POWERS, David** [GB/GB]; Raines Business Centre, Raines House, Denby Dale Road, Wakefield, West Yorkshire WF1 1HR (GB).

(74) Agent: **ROBINSON, Ian, Michael**; Appleyard Lees, 15 Clare Road, Halifax HX1 2HY (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

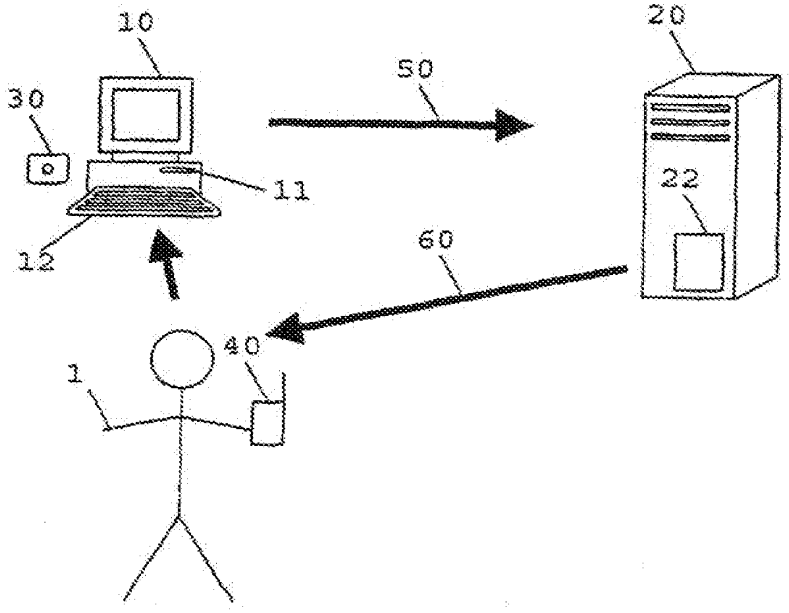
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

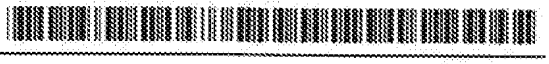
[Continued on next page]

(54) Title: USER IDENTITY VERIFICATION SYSTEM



(57) Abstract: A user identity verification method and apparatus having improved security characteristics are provided. The method and apparatus are suitable for use in a system comprising a client terminal (10) coupled to a server (20) by a first communication medium (50). A user (1) supplies a token (30) comprising first identification information to the client terminal (10), and also supplies identification information such as a memorised username. The supplied first identification information is transmitted over the first communication medium (50) from the client terminal (10) to the server (20). The server verifies that the first identification information corresponds to a stored user profile and then sends a second identification information to the user over a second communication medium (60, 40) such as a GSM network (60) to the user's mobile telephone (40). The user supplies the second identification information to the server (20) via the client terminal (10) and the user's identity is verified at the server according to presentation of the second identification information.

WO 02/084456 A2



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

User Identity Verification System

The invention relates in general to the field of user identity verification. In particular, the invention relates to a method and apparatus for user identification in a client-server system.

In the field of computer systems, it is often desired to verify a user's identity, as user identity verification is important to maintain secure systems. Once a user's identity has been verified, an appropriate level of access can be allowed. In addition to allowing access, knowledge of a user's identity allows that user's browsing and/or other habits to be monitored.

Common user identity verification systems are based on passwords that are memorised by the user. Such systems may be subverted if the memorised information becomes publicly available. Another problem associated with passwords for user identity verification is that a user may require passwords for a number of separate computer systems, and therefore has to remember not only a number of passwords, but also which password corresponds to which computer system. This can lead to a user adopting a common password for all computer systems. Having a single universal password poses a considerable increase in risk of a security breach at all the systems due to the increased likelihood of the password becoming publicly available, and public awareness that one password may permit access to more than one separate computer system. Other more sophisticated forms of subvision exist, such as local or remote monitoring of key storkes or screen displays.

A known alternative user identity verification technique involves the possession of a token, such as a card comprising identification information. The holder of the token can be identified as an authorised user. One example of this type of system is described in the International Application WO 00/62249 in which the token comprises an optical disc or a smartcard disc. However, cards can be stolen or duplicated, allowing unauthorised and/or unidentifiable users to access otherwise secure computer systems.

An aim of the present invention is to provide a method and apparatus for verifying identity of a user in a manner which is reliable and which is not vulnerable to subversion. Preferred embodiments of the present invention aim to address the problems of the prior art mentioned above.

According to a first aspect of the present invention there is provided a method of user identity verification in a system comprising a client terminal couplable to a server by a first communication medium, the method comprising: sending a first identification information over the first communication medium from the client terminal to the server; verifying, at the server, that the first identification information corresponds to a stored user profile; returning a second identification information to a user over a second communication medium according to the stored user profile; sending the second identification information to the server via the client terminal; and verifying user identity, at the server,

according to presentation of the second identification information.

According to a second aspect of the present invention there is provided a user identity verification apparatus comprising: a server comprising a user profile store; a client terminal coupled to a server by a first communication medium; a second communication medium coupled to the server for supply of second identification information to a user, the client terminal being arranged in use to receive the first identification information, and to supply the first identification information over the first communication medium to the server; the server being arranged to verify that the first identification information correspond to a user profile in the user profile store and to supply a second identification information to the user over the second communication medium according to the stored user profile; the client terminal being arranged to receive the second identification information from the user and to supply the second identifier information to the server; and the server being arranged to verify user identity according to presentation of the second identification information.

Preferably, the first identification information includes any one of a username, a memorised access code, information read from a token, or any combination thereof.

Preferably, the first communication medium is different from the second communication medium.

Preferably, the third identification information is supplied to the user over the second communication medium through a mobile communication device.

Preferably, the second identification information is transmitted from the client terminal to the server over the first communication medium.

Preferably, the first identification information is derived from at least one second identification information supplied to a user previously.

Preferably, the first information includes a plurality of second identification information supplied to a user previously, and stored on a token.

Preferably, the token is a removable storage device.

Preferably, the second identification information sent to the user over the second communication medium is regenerated by the server.

For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawing in which:

Figure 1 shows a preferred apparatus for user identity verification; and

Figure 2 shows a flowchart illustrating a preferred method for user identity verification.

Figure 1 shows a preferred apparatus for verifying identity of a user 1. The apparatus comprises a client terminal 10 coupled to a server 20 over a first communication link 50. The server 20 is also coupled to a second communication link 60. The first communication link 50 is ideally different to the second communication link 60. For example, the first communication link 50 comprises a computer network such as a local area or wide area network, a virtual private network, or a more open communication link such as the internet. The second communication link is, for example, a telecommunications network, suitably a wireless telephony network or cellular telephony network. Most preferably the second communication link 60 is a GSM cellular network capable of carrying short messages (SMS).

The apparatus of Figure 1 comprises a user profile store 22 at a suitable verification point. In this example it is convenient for the server 20 to comprise the user profile store 22, although it is possible for the user profile store 22 to be remote from the server 20.

It is desired to verify the identity of a user 1 who wishes to gain access to the apparatus, through the client terminal 10. Here, the client terminal 10 is any suitable form of computing platform, such as a desktop computer or mobile computing device such as a laptop or palmtop computer.

Figure 2 shows a preferred method for verifying user identity, for use with the apparatus of Figure 1.

Initially, the client terminal 10 receives first identification information. Suitably, the first identification information is supplied to the client terminal 10, such as by the user 1 typing a user name and/or memorised access code into a keyboard input device 12 of the client terminal 10.

At step 201, the first identification information is sent from the client terminal 10 to the server 20 over the first communication link 50.

At step 202, the server 20 uses the received first identification information to retrieve a user profile from the user profile store 22. This provides a preliminary identification of the user 1. The server 20 then generates a second identification information, which is returned over the second communication link 60, to reach the user 1, at step 203.

The second identification information is transferred to the client terminal 10, such as by the user 1 typing the second identification information into a keyboard input device 12 of the client terminal 10.

At step 204, the client terminal 10 sends the second identification information back to the server 20, over the first communication link 50.

At step 205, the server 20 verifies the identity of the user 1 based on the received second identification information.

Referring again to Figure 1, ideally the second communication link 60 is a message transmission system such as an SMS system for use on GSM cellular networks. Hence, the second identification information is received by the user 1 such as by using a mobile communications device 40, i.e. a mobile phone.

Advantageously, sending the second identification information to the user's mobile phone 40 according to a predetermined user profile in the user profile store 22, allows increased certainty as to the user's identity. Most users tend to carefully guard their mobile communication device 40 and will notice if it is stolen or subject to subversion. Hence, the user will take precautions to avoid unauthorised use of their mobile communication device 40. By sending the second identification information through the mobile communication device, possession of the mobile communication device 40 allows a high degree of trust to be placed in the user's identity.

As a further enhancement of the present invention, it is preferred that the first identification information is provided at least in part from a token 30. Suitably, the token 30 is readily portable and may be carried by the user 1. The user presents the token 30 to a token reader 11 of the client terminal 10. The token reader 11 extracts the first identification information from the token 30.

In this embodiment, the first identification information may come only from the token 30. Alternatively, the first identification information can be

formed by taking identification information from the token 30, and from a user input such as a user name and/or memorised access code.

The first identification information is received and checked by the server 20, and is used to extract a user profile from the user profile store 22. Suitably, the user profile store 22 contains information which allows a message to be sent over the second communication link 60 to reach the user 1, suitably at their mobile communication device 40. For example, the user profile store contains a predetermined mobile telephone number of the mobile communication device 40.

Suitably, the second identification information is in the form of a password that is randomly generated by the server 20. In an example embodiment, the randomly generated password contains a short string (e.g. eight to twelve characters) containing a sequence of letters and numbers. The user 1 may then easily manually transfer the password from their mobile communication device by typing the password into a keyboard input device of the client terminal 10. Alternatively the password can be automatically transferred from the mobile communication device 40 to the client terminal 10, such as by a short range infra-red communication link.

Any suitable event can be used to trigger the generation of a password by the server 20, e.g. the expiry of a particular time period such as seven days. The trigger may be specific to a particular user, or can cover a small or large group of users to allow mass renewal of passwords conveniently through software administration.

In preferred embodiments, the token 30 is a removable storage medium such as a smart card, or preferably a CD or DVD format storage medium. Ideally, the token 30 comprises an updateable or re-writable storage medium such as a CD-RW or a re-writable DVD. This provides an additional layer of security, as the client terminal 10 can record passwords from previous occasions onto the token 30, i.e. record an incremental identity derived from the previous passwords. The client terminal 10 can then transmit the incremental token identity back to the server 20 via the first communication link 50, and these can also be checked against a list contained in the user profile store 22. Only if the server 20 is satisfied that the first identification information comprising the incremental identity read from the token 30 matches a stored profile in the user profile store 22 is a new password transmitted to the mobile communication device 40 of the user 1. This makes the cloning of tokens a less effective way to defeat the user identity verification system, since a cloned token will become out of date as soon as the real token 30 is used. Furthermore, other security coding can be included with the first identification information on the token 30. The other security coding can also be regenerated and stored on the token 30 to add a yet further layer of security.

The token 30 suitably stores operating software which allows the identity verification system to run on the client terminal 10. Advantageously, by inserting the token 30 into any suitable computer terminal 10, the user 1 is able to operate the identity verification system.

Token 30 can also store other information such as promotional and advertising material. The identification information stored by the token 30 and/or the other information can be strongly encrypted. In yet further embodiments, the token 30 and the mobile communication device 40 can be incorporated into a single unit. Furthermore, the token 30 can in alternative embodiments further comprise a magnetic strip and/or a microprocessor chip to enable a single token 30 to be used for identification in a number of other existing systems. The token may include other visible identification information, such as a photograph identity.

It will be appreciated that the user identity verification system described herein is able to operate at a number of different levels of security. Advantageously, a system administrator is able to select appropriate levels of security according to the needs of particular user or group of users. For some purposes it may be sufficient simply for possession of the token 30 to be an adequate mechanism for identifying the user 1. When a more secure system is desired, the transmission of first and second identification information, via the first and second communication links 50, 60, allows a higher degree of certainty. In a still more secure mode, possession of both the token 30 and the mobile communication device 40 is required. In a still higher security mode, a memorised user name or memorised access code is required, which avoids subversion in the event that the token 30 and the mobile communication device 40 are stolen. Hence, it is very unlikely that all of the communication device 40, the token 30 and the memorised information will be subverted simultaneously.

The method and apparatus for user identify verification described above has many practical applications. As one example, the system is useful in the field of banking, both for identification at cash machines (automatic teller machines), and for internet banking. As another example, the user identification system can be used to control access to buildings in combination with electronic locking mechanisms. Further example applications include authentication for pay-per-view broadcasting systems, or access to a private electronic messaging system.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise,

each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Claims

1. A method of user identity verification in a system comprising a client terminal couplable to a server by a first communication medium, the method comprising:

sending a first identification information over the first communication medium from the client terminal to the server;

verifying, at the server, that the first identification information corresponds to a stored user profile;

returning a second identification information to a user over a second communication medium according to the stored user profile;

sending the second identification information to the server via the client terminal; and

verifying user identity, at the server, according to presentation of the second identification information.

2. A user identity verification apparatus comprising:

a server comprising a user profile store;

a client terminal coupled to a server by a first communication medium;

a second communication medium coupled to the server for supply of second identification information to a user,

the client terminal being arranged in use to receive the first identification information, and to supply the first identification information over the first communication medium to the server;

the server being arranged to verify that the first identification information correspond to a user profile in the user profile store and to supply a second identification information to the user over the second communication medium according to the stored user profile;

the client terminal being arranged to receive the second identification information from the user and to supply the second identifier information to the server; and

the server being arranged to verify user identity according to presentation of the second identification information.

3. The method or apparatus of claims 1 or 2, wherein the first identification information includes any one of a username, a memorised access code, information read from a token, or any combination thereof.

4. The method or apparatus of any preceding claim wherein the first communication medium is different from the second communication medium.

5. The method or apparatus of any preceding claim wherein the third identification information is supplied to the user over the second communication medium through a mobile communication device.

6. The method or apparatus of any preceding claim wherein the second identification information is transmitted from the client terminal to the server over the first communication medium.

7. The method or apparatus of any preceding claim, wherein the first identification information is derived from at least one second identification information supplied to a user previously.

8. The method or apparatus of claim 7, wherein the first information includes a plurality of second identification information supplied to a user previously, and stored on a token.

9. The method or the apparatus of any of claims 3 to 9, wherein the token is a removable storage device.

10. The method or apparatus of any preceding claim wherein the second identification information sent to the user over the second communication medium is regenerated by the server.

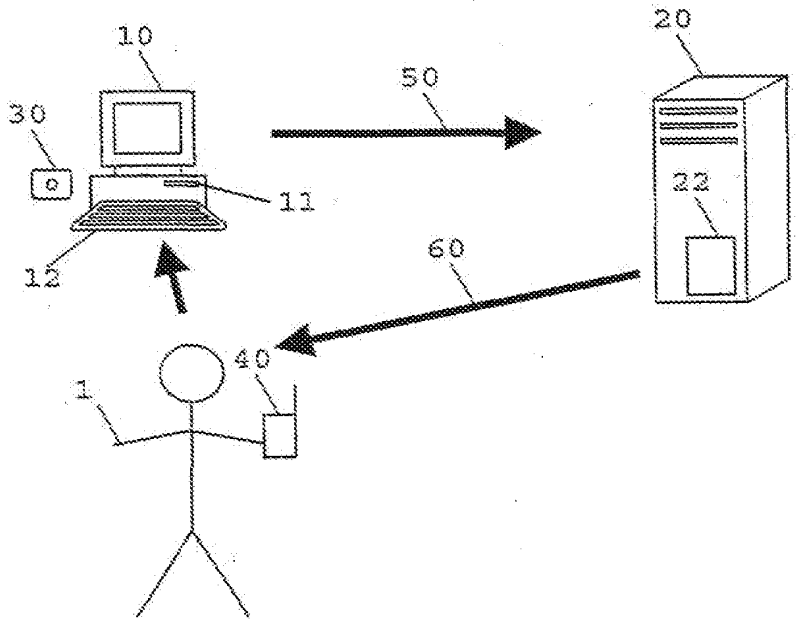


Fig. 1

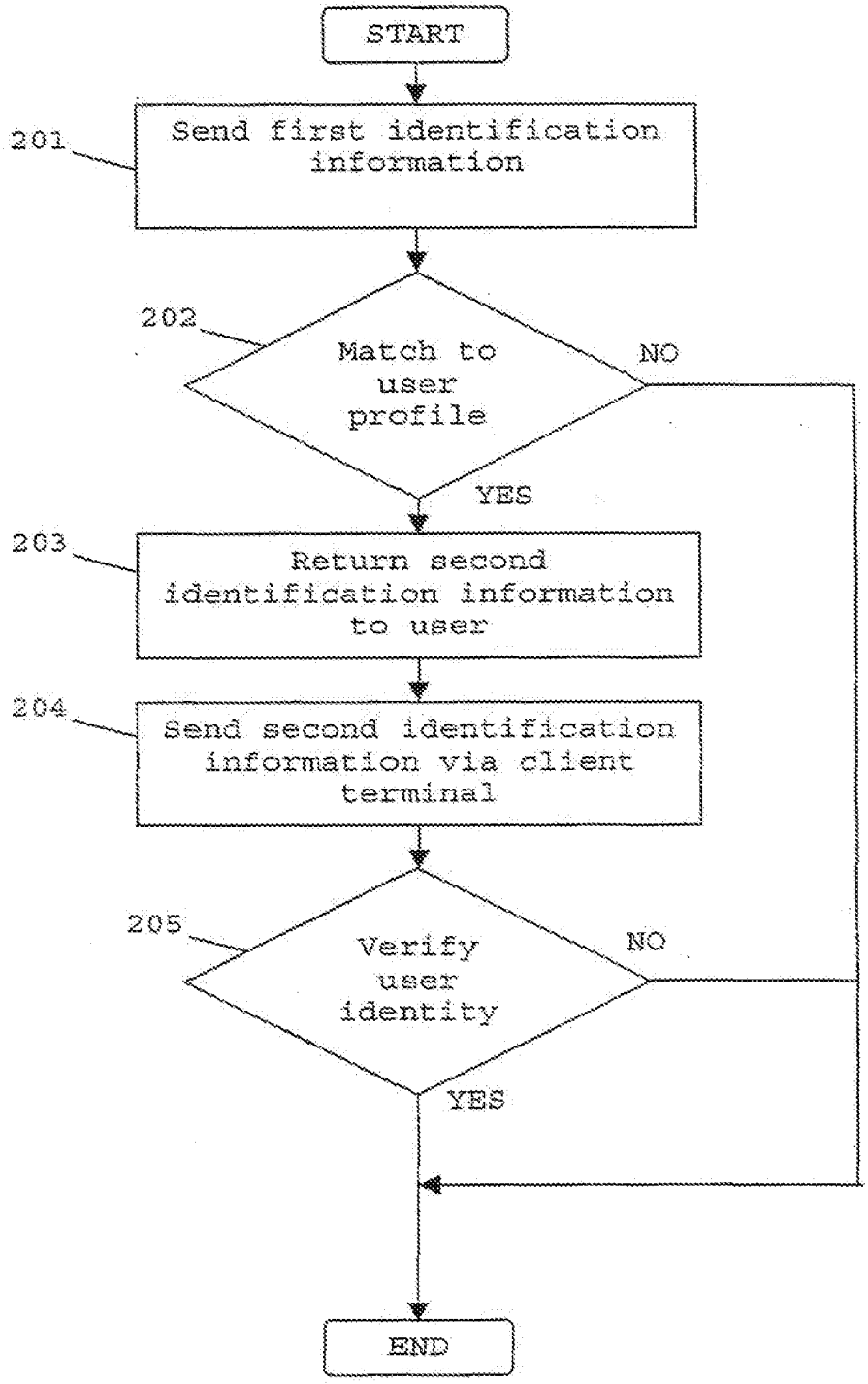

START
201
Send first identification information
202
Match to user profile
NO
YES
203
Return second identification information to user
204
Send second identification information via client terminal
205
Verify user identity
NO
YES
END

Fig. 2

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/084456 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB02/01645

(22) International Filing Date: 11 April 2002 (11.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0109200.6	12 April 2001 (12.04.2001)	GB
0111528.6	11 May 2001 (11.05.2001)	GB
0126583.4	6 November 2001 (06.11.2001)	GB
0126929.9	9 November 2001 (09.11.2001)	GB

(71) Applicant *(for all designated States except US)*: **NET-DESIGNS LIMITED** [GB/GB]; Raines Business Centre, Raines House, Denby Dale Road, Wakefield, West Yorkshire WF1 1HR (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **POWERS, David** [GB/GB]; Raines Business Centre, Raines House, Denby Dale Road, Wakefield, West Yorkshire WF1 1HR (GB).

(74) Agent: **ROBINSON, Ian, Michael**; Appleyard Lees, 15 Clare Road, Halifax HX1 2HY (GB).

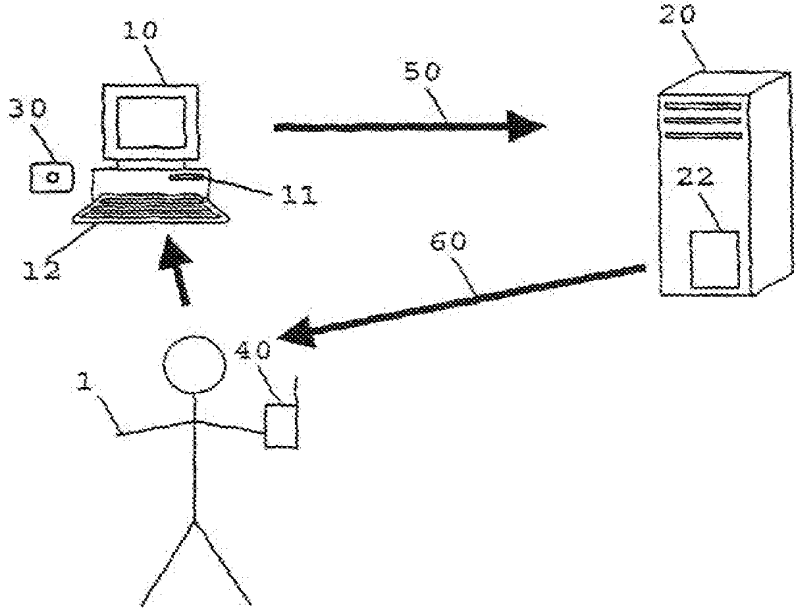
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

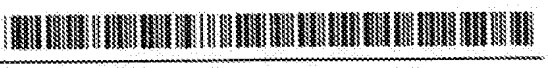
[Continued on next page]

(54) Title: USER IDENTITY VERIFICATION SYSTEM



(57) Abstract: A user identity verification method and apparatus having improved security characteristics are provided. The method and apparatus are suitable for use in a system comprising a client terminal (10) coupled to a server (20) by a first communication medium (50). A user (1) supplies a token (30) comprising first identification information to the client terminal (10), and also supplies identification information such as a memorised username. The supplied first identification information is transmitted over the first communication medium (50) from the client terminal (10) to the server (20). The server verifies that the first identification information corresponds to a stored user profile and then sends a second identification information to the user over a second communication medium (60, 40) such as a GSM network (60) to the user's mobile telephone (40). The user supplies the second identification information to the server (20) via the client terminal (10) and the user's identity is verified at the server according to presentation of the second identification information.

WO 02/084456 A3



before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(88) Date of publication of the international search report:
30 October 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/GB 02/01645

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 95 19593 A (KEW MICHAEL JEREMY ;LOVE JAMES SIMON (GB)) 20 July 1995 (1995-07-20) abstract page 1, line 20 -page 2, line 3 page 6, line 28 - line 33 page 7, line 28 -page 8, line 10 page 9, line 27 -page 11, line 4 figure 1	1-6,9,10
X	EP 0 844 581 A (VENEKLASE BRIAN J) 27 May 1998 (1998-05-27) abstract page 3, column 3, line 54 -page 3, column 4, line 15 figure 6	1-6,10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2003	02/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Segura, G

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Interna application No
PCT/GB 02/01645

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 1 107 089 A (CONNECTOTEL LTD) 13 June 2001 (2001-06-13) the whole document	1-6,10
A	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 (1991-10-22) abstract column 4, line 27 -column 4, line 61 column 6, line 35 -column 6, line 68	7,8
A	US 6 148 404 A (YATSUKAWA NAONOBU) 14 November 2000 (2000-11-14) abstract	7,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat application No
PCT/GB 02/01645

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9519593 A	20-07-1995	AU 1390395 A WO 9519593 A1 GB 2300288 A	01-08-1995 20-07-1995 30-10-1996
EP 0844551 A	27-05-1998	US 5881226 A EP 0844551 A2	09-03-1999 27-05-1998
EP 1107089 A	13-06-2001	EP 1107089 A1	13-06-2001
US 5060263 A	22-10-1991	NONE	
US 6148404 A	14-11-2000	JP 10336169 A	18-12-1998

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 844 551 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.05.1998 Bulletin 1998/22

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **97890210.4**

(22) Date of filing: **22.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **26.10.1995 US 738897**

(71) Applicant: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(72) Inventor: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(74) Representative: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

Remarks:
A request for correction (exchanging the contents of figure 1 with figure 2 and vice versa) has been filed pursuant to Rule 88 EPC. A decision on the request will be taken during the proceedings before the Examining Division (Guidelines for Examination in the EPO, A-V, 3.).

(54) Computer security system

(57) Several embodiments of computer security systems are described and which are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream. In one embodiment, the security system comprises: an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel, analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to a code; and a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means; and a notification means for receiving said code and for notifying said authorized individual of the identity of said code.

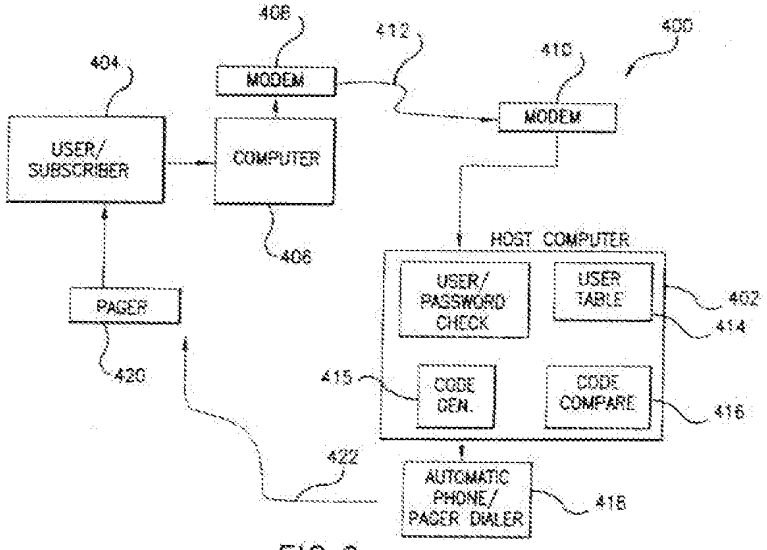


FIG.6

EP 0 844 551 A2

Description

1. Field of the Invention

The present invention relates to a security and/or access restriction system and, in one embodiment, to a security and/or access restriction system which is adapted to grant only authorized users access to a computer system and/or to certain data which may be resident within the computer system and/or resident within a communications channel and/or other communications medium.

2. Background of the Invention

In recent years, computers have proliferated in all parts of worldwide society, including but not limited to, banking, financial services, business, education, and various governmental entities. For instance and without limitation, these computer systems allow individuals to consummate financial transactions, to exchange confidential scientific and/or medical data, and to exchange highly proprietary business planning data. Hence, these computer systems require and/or allow very sensitive and confidential data to be stored and transmitted over great geographic distances.

Moreover, the rise of multinational communications networks, such as the publicly available Internet communications system, has truly made the world a smaller place by allowing these computers, separated by great geographic distances, to very easily communicate and exchange data. In essence, these worldwide communications channels/networks, sometimes collectively referred to as "the Information Superhighway" have electronically connected the peoples of the world - both the good and the very bad.

That is, while these computer systems have increased efficiency and greatly changed the manner in which we work and interact, they have been especially prone to unauthorized "break-ins", viral destruction, and/or unauthorized data modifications. Accordingly, the rather sensitive and confidential data which is stored and used within these computer systems and transmitted between these computer systems has been the target of attack by people known as "hackers" and by high level and very sophisticated espionage and industrial spies. Computer access security and data transmission security has recently come to the forefront of importance and represents one of the great needs of our times.

Many attempts have been made to create and utilize various techniques (hereinafter the term "technique" as used and/or employed in this Application refers to any combination of software, hardware, and/or firmware which comprise an apparatus and a methodology whose components cooperatively achieve an overall security objective) to "ensure" that only authorized users are allowed to gain access to these respective computer systems. These prior techniques, while somewhat effective, suffer from various drawbacks.

For example, one such prior computer system security technique comprises the use of predetermined "passwords". That is, according to this security technique, each computer system has a list of authorized passwords which must be communicated to it before access is given or allowed. In theory, one or more "trusted" system administrators distribute these "secret" passwords to a group of authorized users of a computer system. The "secret" nature of the passwords, in theory, prevents unauthorized users from accessing the computer system (since presumably these unauthorized users do not have the correct passwords). This technique is not very effective since oftentimes those authorized individuals mistakenly and unwittingly expose their password to an unauthorized user Moreover, this technique of data security may be easily "broken" by a "hacker's" deliberate and concentrated attempt at automatically inputting, to the targeted computer, hundreds and perhaps thousands of passwords until an authorized password is created.

In addition to the prior password technique other, more sophisticated access techniques are known and used. For example, there are known techniques which require the possession of a physical object or feature, such as "access cards" which are "read" by a card reading device and biometric authentication techniques (e. g. requiring the initial input of such authorized user physical characteristics as fingerprints and eye patterns and the later comparison of these input patterns to those of a "would-be" user). Both of these prior techniques are relatively complicated, are relatively costly, and are prone to error, such as and without limitation, mistaken unauthorized entry due to their complexity. These techniques are also prone to unauthorized entry by use of counterfeit and/or stolen cards, objects, and fingerprint readers. Other prior data security techniques, such as encryption, attempt to prevent unauthorized use of transmitted data or unauthorized access to a computer system by modifying and/or changing the transmitted data in a certain manner, and/or requiring the transmission and receipt of modified data before access is granted. While somewhat effective, these prior encryption techniques are relatively costly and complicated and require one or more known "encryption keys" which are in constant exchange between users and which are themselves susceptible to theft and/or inadvertent disclosure. Furthermore, the best-known and perhaps strongest encryption algorithm is proprietary and cannot be used without a costly license. Moreover, since the encrypted message still provides all of the transmitted data, in some form, it is still possible for one to gain access to the entire data stream by "breaking the encryption code". Since no encryption algorithm is ever considered "unbreakable", encryption is not considered to be a "foolproof" security solution.

There is therefore a need to provide a technique to substantially prevent the unauthorized access to one or

more computer systems and which overcomes the various drawbacks of these afore-described prior techniques. There is also a need to provide a technique to substantially prevent the unauthorized interception and use of transmitted data and which overcomes the various drawbacks of the prior art. Applicant's invention(s) seek and do meet these needs. Applicant's invention, in one embodiment, achieves these objectives by splitting the data into a plurality of separate communication channels, each of which must be "broken" for the entire data stream to be obtained. In essence, in this embodiment of Applicant's invention, cooperatively form the entire message. The splitting of the data in this manner may also "fool" the would be data thief into believing that he or she has obtained all of the data when, in fact, only several communication channels are obtained.

SUMMARY OF THE INVENTION

While a number of "objects of the invention" are set forth below, it should be realized by one of ordinary skill in the art that the invention(s) are not to be limited, in any manner, by these recited objects. Rather, the recited "objects of the invention" are to be used to place Applicant's various inventions in proper overall perspective and to enable the reader to better understand the manner in which Applicant's inventions are to be made and used, especially in the preferred embodiment of Applicant's invention. Accordingly, the various "objects of the invention" are set forth below:

It is a first object of the present invention to provide a technique to substantially ensure that only authorized users gain access to a computer system.

It is a second object of the invention to provide a technique to substantially ensure that only authorized users gain access to a computer system and which overcomes the various previously delineated drawbacks of the prior computer system security techniques.

It is a third object of the invention to provide a technique to substantially ensure that only authorized users have access and use of certain transmitted data appearing, for example, within a data stream.

It is a fourth object of the invention to provide a technique to substantially ensure that only authorized users have access and use of certain transmitted data and/or certain hardware, software, and/or firmware which cooperatively form and/or comprise a computer system, and that this technique overcomes the various previously delineated drawbacks of the prior techniques.

According to a first aspect of the present invention, a security system is provided. Particularly, the security system is adapted to be used in combination with a computer and to only grant an authorized individual access to the computer. The security system comprises, in one embodiment, password means for receiving a password by use of a first communications channel; and code generation means, coupled to said password means, for generating a code by use of a second communications channel, and to allow that individual access to the computer system only if that individual generates and communicates the code to the code generation means.

According to a third aspect of the present invention, a method is provided for use with a computer and effective to substantially prevent an unauthorized user from accessing the computer. The method comprises, in one embodiment, the steps of assigning a password to the user; receiving the password by use of a first communications channel; generating a code in response to the received password; transmitting the code by use of a second communications channel to the user; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer.

According to a fourth aspect of the present invention, a security system is provided to grant an authorized individual access to a secured stream of data bits. In one embodiment, the data security system comprises a data stream dividing means for receiving said stream of data bits and dividing said stream of data bits into a plurality of sub-streams; transmitting means for transmitting said sub-streams in a predetermined order over a communication channel; and a decoding means for receiving said sub-streams and for recombining said received sub-streams to create said secured stream of data bits.

Further objects, features, and advantages of the present invention will become apparent from a consideration of the following description, the appended claims, and/or the appended drawings. It should further be realized by one of ordinary skill in the art that the previously delineated objects and aspects of the invention are for illustration purposes only and are not to be construed so as to limit the generality of the inventions and/or to limit the interpretation to be given to the various appended claims. Moreover, it should also be realized by those of ordinary skill in the art that the term "communications channel" as used throughout this Application refers to any physical and/or electromagnetic means or method of transferring and/or communicating information from one or more sources to one or more receivers. Moreover, the term "communications channel" should be given the broadest known interpretation covering any method and/or medium which facilitates the transfer of information and/or over which such information is transferred.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller and more complete understanding of the nature and objects of the present invention, reference should be had to the following drawings wherein:

FIG. 1 is a block diagram of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred security techniques of the invention;

FIG. 2 is a block diagram of another embodiment of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention;

FIG. 3 is a block diagram of yet another embodiment of a security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention;

FIG. 4 is a block diagram of another embodiment of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention;

FIG. 5 is a schematic diagram of a password table used by the computer security systems shown in Figures 1 and 2; and

FIG. 6 is a block diagram of one embodiment of the preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to Figure 1, there is shown a block diagram of a computer security system 10, made in accordance with the principles of the preferred embodiment of the invention and adapted for use in combination with computer 80. More particularly, computer security system 10 selectively allows communication and/or data processing access to computer 80 in a manner which is technically described throughout the remainder of this Application. As shown, security system 10 includes an "analyzing means" 12 and a "random code generating means" 14.

In one embodiment of the preferred embodiment of the invention, analyzing means 12 comprises one or more software subroutines which are adapted to execute upon and/or within computer 80. Alternatively, analyzing means 12 may comprise a microprocessor and/or similar type of computer which is adapted to operate under stored program control in the manner set forth in this Application. One example of another type of computer operating under stored program control and which may be used by the preferred embodiment of the invention is shown and described within chapter eight of the text entitled Advanced Computer Architecture: Parallelism Scalability Programmability, which was authored by Kai Hwang, which is published by McGraw-Hill, Inc., which has a library reference number of ISBN 0-07-031622-8, and the entire text of all of the chapters of which are fully and completely incorporated herein by reference, word for word and paragraph for paragraph. In either embodiment, analyzing means 12 receives and compares at least two "sets" or streams of data. Should the individually received "sets" match, analyzing means 12 generates and communicates an "access granted" command to computer 80, allowing individual 18 access to the computer 80 Moreover, random code generating means 14 may similarly comprise a conventional pseudo-random number generator which may be constructed or developed on one or more software subroutines which reside and operate/execute upon and/or within computer 80 or may comprise a microprocessor and/or similar type of computer which operates under stored program control.

In operation, individual 18, desiring access to and within computer 80 utilizes a first communication channel 82 (e.g. a first telephone line, radio channel, and/or satellite channel) and communicates, by use of his or her voice or by use of a computer 19 a first password to analyzing means 12. Analyzing means 12 then checks and/or compares this first received password with a master password list which contains all of the authorized passwords associated with authorized entry and/or access to computer 80.

As shown in Figure 5, in the preferred embodiment of the invention, analyzing means 12 contains a master password list 200 having a first column of entries corresponding to authorized passwords necessary to gain access to computer 80. Moreover, as further shown in Figure 5, each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user.

If the received password matches an entry of the master password list, analyzing means 12 generates a command, by means of connecting bus 17 or software message or function call to random code generating means 14 and causes the random code generation means 14 to generate a substantially random and/or pseudo-random number or code, of programmable length, and to transmit the number and/or code, by means of a second communications channel 84, to the individual 85 associated with the received password 202 in the master password list. That is, as should be apparent to one of ordinary skill in the art, code generation means 14 includes both a random number generator and a conventional and commercially available communications interface (e.g. modem and/or telephone/pager interface), allowing the generated pseudo-random code to be generated or communicated over a wide variety of mediums.

Further, it should be apparent that individual 85 may or may not be the same person as individual 18 , if individual 18 was the individual identified in the master password list (e.g. "was authorized"), that individual 18 receives the pseudo-random number and transmits the number to the analyzing means 12, by means of communications channel 82. Once the pseudo-random number is received by the analyzing means 12, from channel 82, it is compared with the number generated by generation means 14. If the two codes are substantially the same, entry to computer 80 and/or to a certain part of computer 80 such as, without limitation, the hardware, software, and/or firmware portions of computer 80 is granted to individual 18. For instance, in another em-

bodiment, table 200 of Figure 5 could contain yet another set of entries specifying the directories or portions of computer 80 that the individual 18 was allowed to have access to. In this manner, allowed access to computer 80 would be further restricted to those computer portions which are specified within table 200. It should be apparent to one of ordinary skill in the art that these portions may be different for different users and that each authorized user may have a different portion that may be accessed in an authorized manner.

It should be apparent to one of ordinary skill in the art that Applicant's foregoing computer security technique is a relatively low-cost, but effective technique, for properly ensuring that only authorized users gain access to a computer system, such as computer system 80. That is, Applicant's foregoing computer security embodiment, utilizes two distinct communications channels and a random number generator in order to ensure that an authorized user of a computer system is notified that someone or something is seeking access to the computer system with his or her password. Moreover, Applicant's foregoing invention is very cost effective as it employs substantially "off the shelf" and readily available components. Further, the use of a "secret" password, a "secret" substantially random number, and a "secret" second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art.

Referring now to Figure 6 there is shown a computer system 400 made in accordance with the teachings of the preferred embodiment of the invention and representing one example and/or implementation which is made in accordance with the various teachings of the preferred embodiment of the invention As shown, computer system 400 includes a host computer 402 (corresponding to computer 80 of the system shown in Figure 1) to which a user or other individual 404 (corresponding to individual 18 of Figure 1) desires access to. As further shown in Figure 6, As shown, individual 404, in this implementation example, utilizes a commercially available and conventional computer 406 and a commercially available and conventional modem 408 to communicate with a commercially available and conventional modem 410 by means of a typical communications channel (e. g. a conventional "dial-up" telephone line) 412. Hence, the user 404, in this embodiment, only requires conventional computer equipment. Host computer 402, in this embodiment, requires a conventional and commercially available automatic dialer which is altered, in a known manner, to receive and pass one or more passwords and/or codes as data.

In operation, user 404 dials through and/or by means of his or her computer 406 and modem 408 in the usual and conventional manner to connect and access host computer 402. The host computer 402, using the principles of the preferred embodiment of this invention, answers the requester's call, which occurs over channel 412, and requests and receives the user's identification code. host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402. This comparison, is a match is made, causes the "code generator" software subroutine 415, resident within computer 402, to generate a pseudo-random number code and passes the received code along with the authorized user's pager number to the commercially available and conventional automatic dialer 418. The automatic dialer 418 telephones the conventional and commercially available pager 420 by means of conventional and commercially available communication channel 422 (e.g. voice line) and transmits the code to the user's pager. As this happens, the host computer 402 awaits the reply from the user attempting to gain access to the computer.

The user 404 now enters the code he or she has received from the pager 420 and any timing instructions which, in yet another embodiment of the invention may also be transmitted from computer 402, and sends this password or pseudo-random code back to computer 402 where it is compared within the software subroutine module denoted as "code compare" 416 in Figure 6. If the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.

Referring now to Figure 2, there is shown a second embodiment of a computer security system made in accordance with the teachings of the preferred embodiment of the invention. This second embodiment 20 is substantially similar to system 10 but also includes a timer or "timing means" 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80 or may comprise a microprocessor which operates under stored program control. In one embodiment, timing means 40 comprises a conventional "watchdog timer" as will be apparent to those of ordinary skill in the art.

In operation, timing means 40 records the time at which the first and second passwords are received by analyzing means 12. Timing means 40, in one embodiment which is coupled to analyzing means 12 and code generation means 14 by bus 42 and in another embodiment which is in software communication with means 12 and 14, then compares the times to determine whether the second password was received within a predetermined period or predetermined "window" of time after the first password was received. In the preferred embodiment of the invention, the predetermined period of time is programmable. The predetermined period of time, will typically need to vary according to the nature of the communications medium used by means 14 to notify individual 85 of the value of the generated code. For example, the predetermined period of time would be shorter when communications channel 84 comprises a pager or cellular phone, since the owner has immediate access to the code upon transmission, and longer

when communications channel 84 comprises a voice-mail system which the owner has to affirmatively access to receive the code. If the second password was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g. computer 80). If the second password was received within the predetermined period of time, analyzing means 12 compares it to the code which was previously generated. If the second password is not substantially identical to the previously generated code, analyzing means 12 denies individual 18 entry to the secured domain (e.g. computer 80). If the received password is substantially identical to the code, analyzing means 12 grants individual 18 entry into the secured domain. As will be readily apparent to those of ordinary skill in the art, timing means 40 provides yet a third level of security to computer system 80. Moreover, it should also be apparent to one of ordinary skill in the art that this "predetermined time" may be as short or as small as several milli-seconds or micro-seconds. This is particularly true if, in yet another embodiment of Applicant's invention, the password generated by communication means 14 is received by a computerized device which is adapted to received the password and to generate a new password code in a substantially automatic manner.

Referring now to Figure 3, there is shown a block diagram of a third embodiment of a computer security system made in accordance with the principles of the preferred embodiment of the invention As shown, computer security system 70 is adapted to receive an input data stream 72, comprising in a first embodiment, a plurality of digital data bits 73, which are to be securely transmitted to a distant site. System 70, as further shown, includes a data stream dividing means 74 which in one embodiment comprises a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of received data and places, in a certain predetermined manner (e.g. alternately) some of the received data bits onto the first communications channel 76 and some of the received data bits onto the second communications channel 78. In this manner, one attempting to wrongfully intercept and/or access the data stream 72 would need access to both communications channels 76, 78 and would need to know the dividing algorithm that dividing means 74 utilizes to divide the received data for placement onto channels 76,78. Applicant's third embodiment therefore provides a very high level of data transmission security.

As further shown in Figure 3, in this third embodiment of the invention, security system 70 further includes a decoding means 88 which may comprise a commercially available microprocessor operating under stored algorithmic program control and which contains "mirror image" of the algorithm used to divide the data stream transmitted to it by means 74. In this manner, the data from each of the channels 76,78 is reconstituted onto single channel 89, in substantially the exact same manner that it was received by means 74. In essence, this third embodiment of Applicant's invention allows and/or provides for the "splitting" of a data stream into a plurality of channels in a predetermined manner and the concomitant reconstitution of the data stream once the data has traversed the communications medium. Hence, the embodiment in Figure 3 splits the data stream so that anyone getting access to one of the channels 76, 78 can't reconstruct the data stream because they're missing half or more of the information. If more channels are used, each channel carries far less than one-half the information.

Referring now to Figure 4 there is shown a fourth embodiment of a computer security and/or data transmission system 100 which is made in accordance with the teachings of the preferred embodiment of the invention As shown, system 100 is adapted to receive a plurality of data bits 103 contained in a first communications channel 102. It should be noted that the data contained within this channel 102 is interspersed with a plurality of "non-data" or filler data bits or "material" 104 according to some predetermined and/or randomly varying algorithm (e.g. every third bit space is filler data) by a microprocessor system 106 which is operating under stored program control. The filler data 104 is binary data and cannot be deciphered as "filler" by an unauthorized user. Therefore, even if one were to intercept the transmitted data, one could not decipher or decode the data. System 100 further includes a decoder 110 for the data reception and decodes 202 for the algorithm reception which, in one embodiment, comprises a microprocessor acting under stored program control and which is adapted to "strip off" the "filler" bits and to allow the originally transmitted data to be reconstituted. In this manner, data may be safely transmitted and received in an authorized manner. In yet another embodiment of the invention which is shown in Figure 4, the algorithm which controls the filler pattern and/or the way that the filler data is interspersed within the "regular" data pattern may be periodically changed in a known and predetermined manner. In this embodiment, the filler data is interspersed within the "regular" data according to a varying filler algorithm (e.g. every three bits for the first 99 bits and then every four bits thereafter). In this embodiment, decoder 110 is adapted to "strip" off these filler bits by having prior knowledge (e.g. embedded within a computer program resident within and controlling the decoder) of the varying algorithms which are utilized by system 100. Here, in the embodiment shown in Figure 4, unlike that shown and described with respect to Figure 3, all the data is transmitted on a single channel but is "muddied."

In yet another embodiment of the invention, as shown in Figure 4, a varying data key is transmitted to decoder 110 and/or decoder 202 by microprocessor system 106 by use of a second channel 200. In this manner, a second channel is needed to tell or communicate the manner in which the filler data is interspersed within the regular data so that the decoder 110 may "strip off" the filler data. In this manner, the filler patterns may be

dynamically changed. Hence, this system utilizes dual/multi channel media to communicate the cryptic modulation of the data with filler.

It is to be understood that the invention is not limited to the exact construction or method illustrated and described above, but that various changes and modifications may be made without departing from the spirit and scope of the invention as defined in the following claims.

Claims

1. A security system for use in combination with a computer, said security system comprising:

   An analyzing means for receiving first password, for generating a first signal in response to said received first password, for receiving a first code, for receiving a second code, and for allowing access to said computer only if said first and said second codes are substantially identical and;
   code generation means for receiving said first signal and for generating and communicating said first code to said analyzing means.

2. A method to restrict access to a certain group of individuals to a computer, said method comprising the steps of:

   assigning a unique password to each of said certain group of individuals;
   assigning a telephone number to each of said unique passwords;
   receiving a data stream;
   comparing said data stream to each of said unique passwords identifying one of said unique passwords with said data stream;
   generating and transmitting a first code to said telephone number associated with said one identified password;
   receiving a second code,
   comparing said first and said second codes; and
   allowing access to said computer only is said first and said second codes are substantially identical.

3. A method to securely transmit data comprising the steps of:

   receiving said data;
   distributing said received data into a plurality of communications channels;
   transmitting said distributed data by use of said plurality of communication channels;
   receiving said distributed data,
   and reconstituting said data.

4. A method to securely transmit data having a plurality of bits, said method comprising the steps of:

   interspersing a plurality of filler data bits into said data in a certain pattern;
   transmitting said data and aid interspersed filler data;
   receiving said data and said interspersed filler data;
   and discarding said interspersed filler data.

5. A security system adapted to grant an authorized individual access to secured domain, comprising:

   an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel, analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to code; and
   a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means.

6. The invention according to claim 1 wherein said analyzing means if further comprises a timing means for recording the time that said first password is received and granting access to said secured domain only if said second password is received within a predetermined period of time.

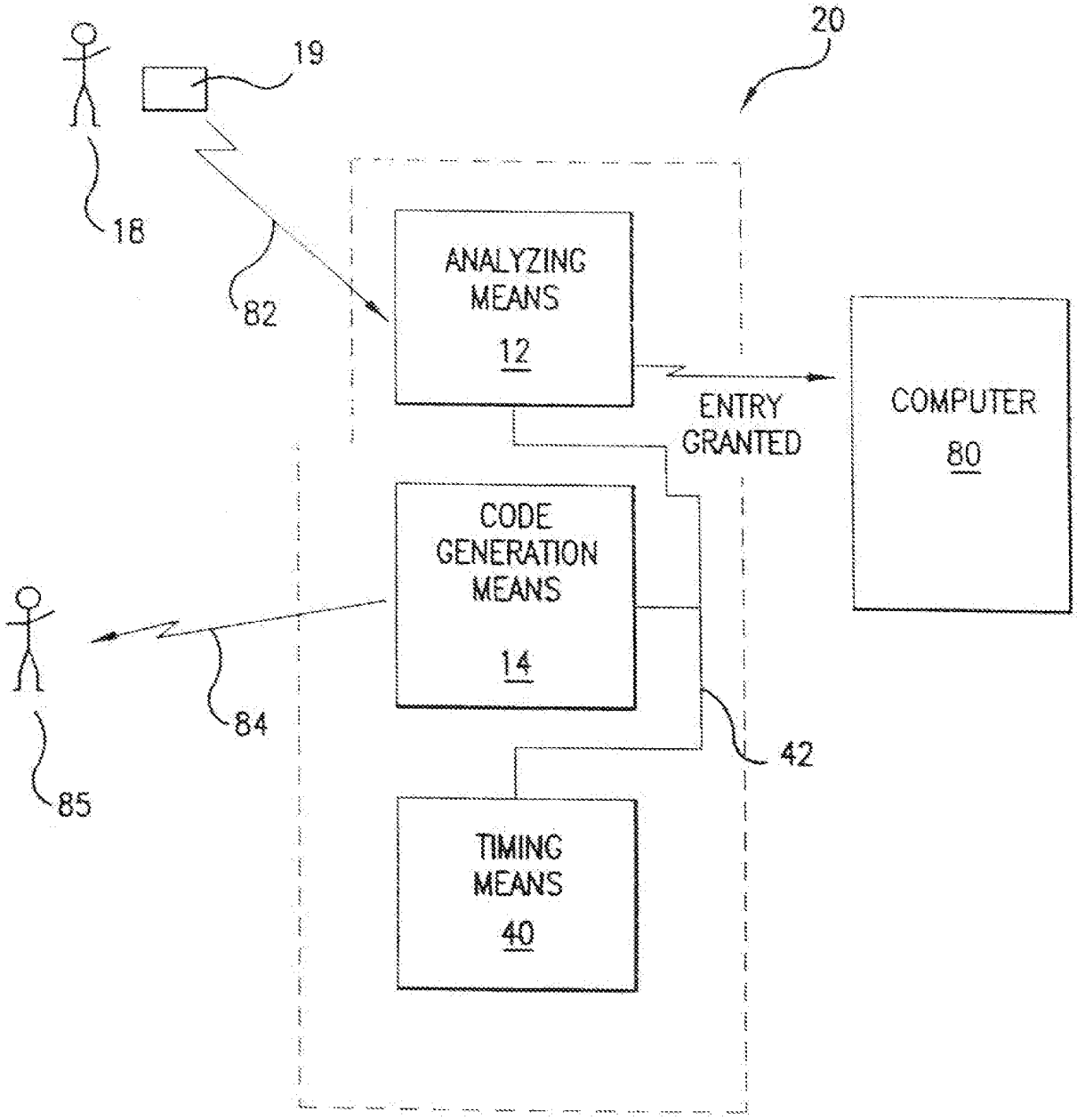

20
19
18
82
ANALYZING MEANS
12
ENTRY GRANTED
COMPUTER
80
CODE GENERATION MEANS
14
84
85
42
TIMING MEANS
40

FIG.1

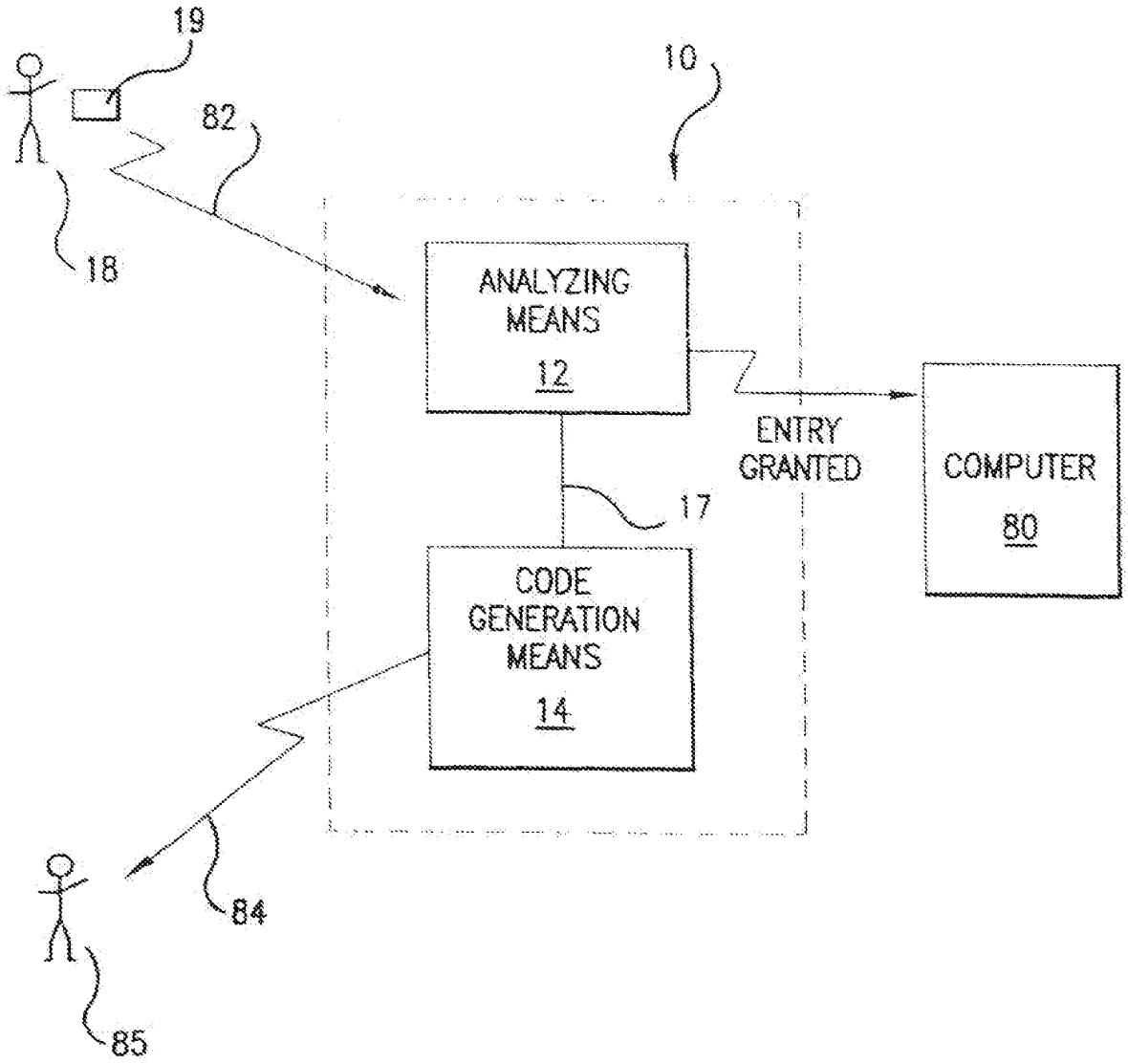

19
10
82
18
ANALYZING MEANS
12
ENTRY GRANTED
COMPUTER
80
17
CODE GENERATION MEANS
14
84
85

FIG.2

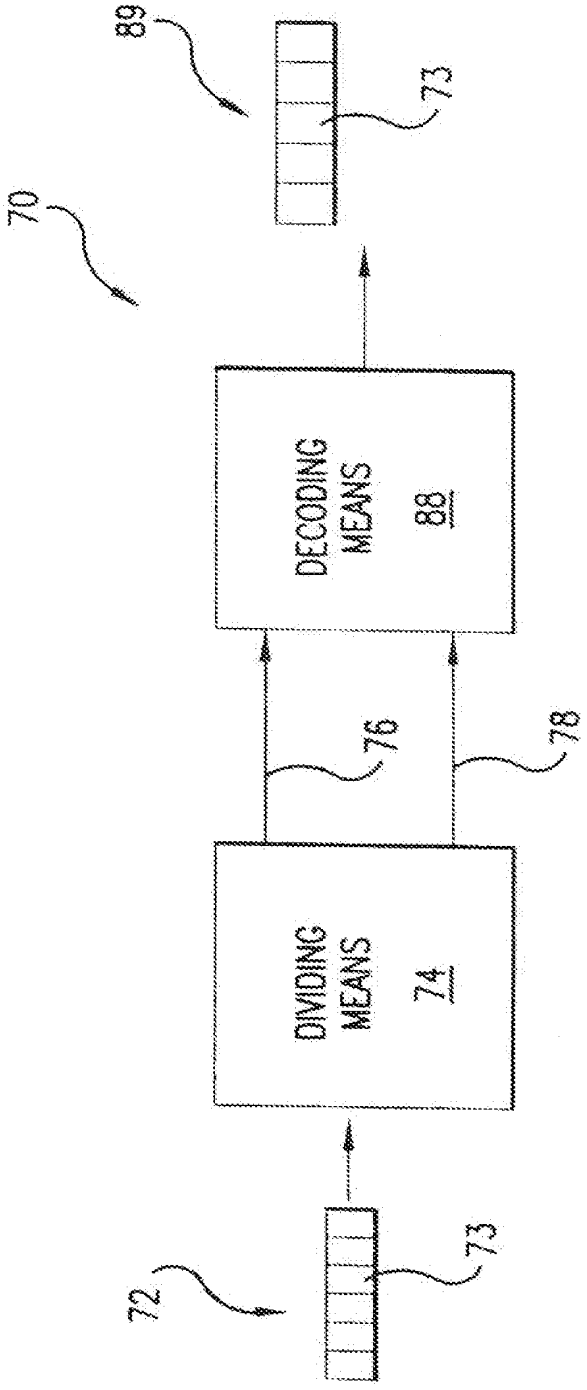


FIG.3

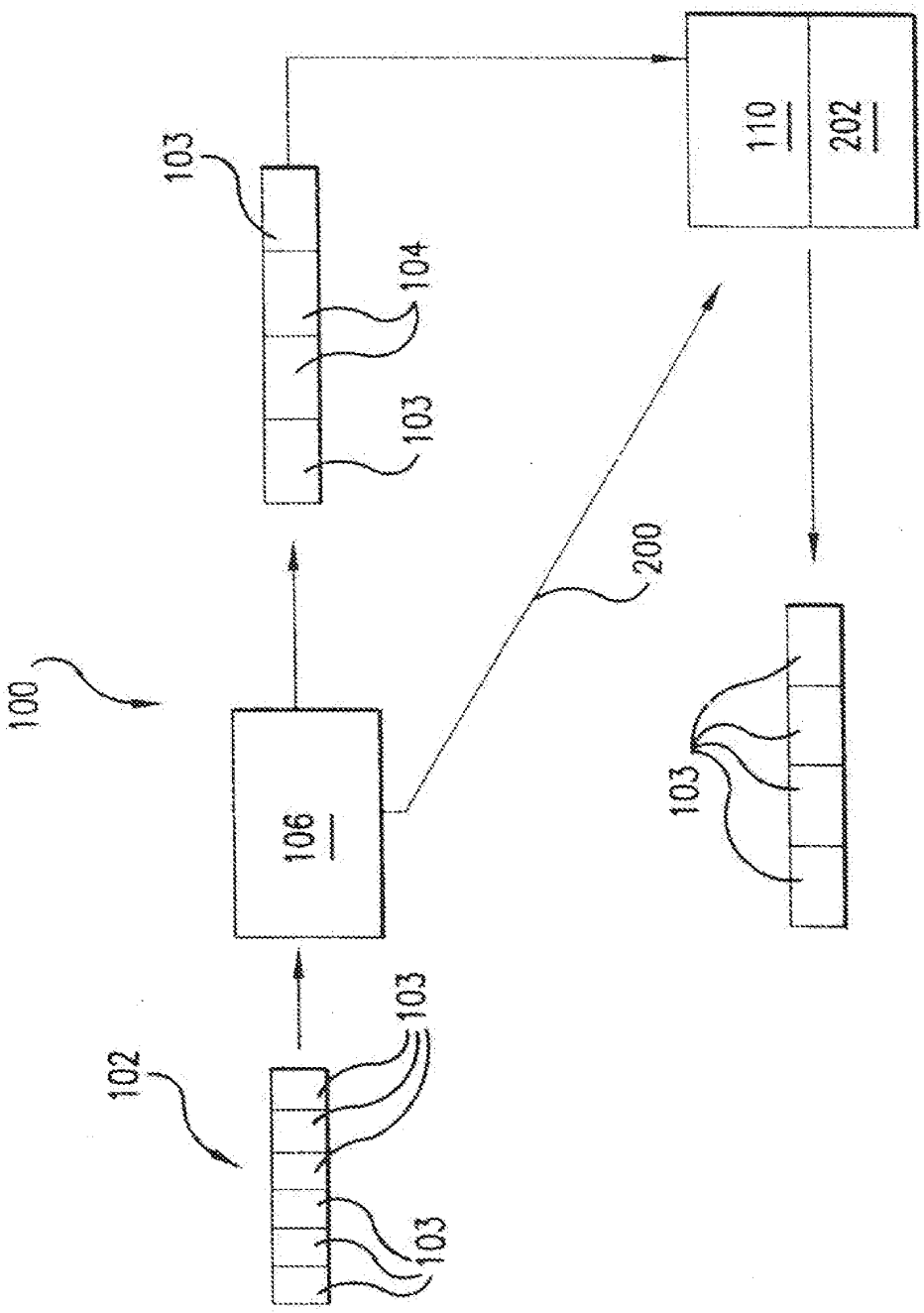


FIG. 4

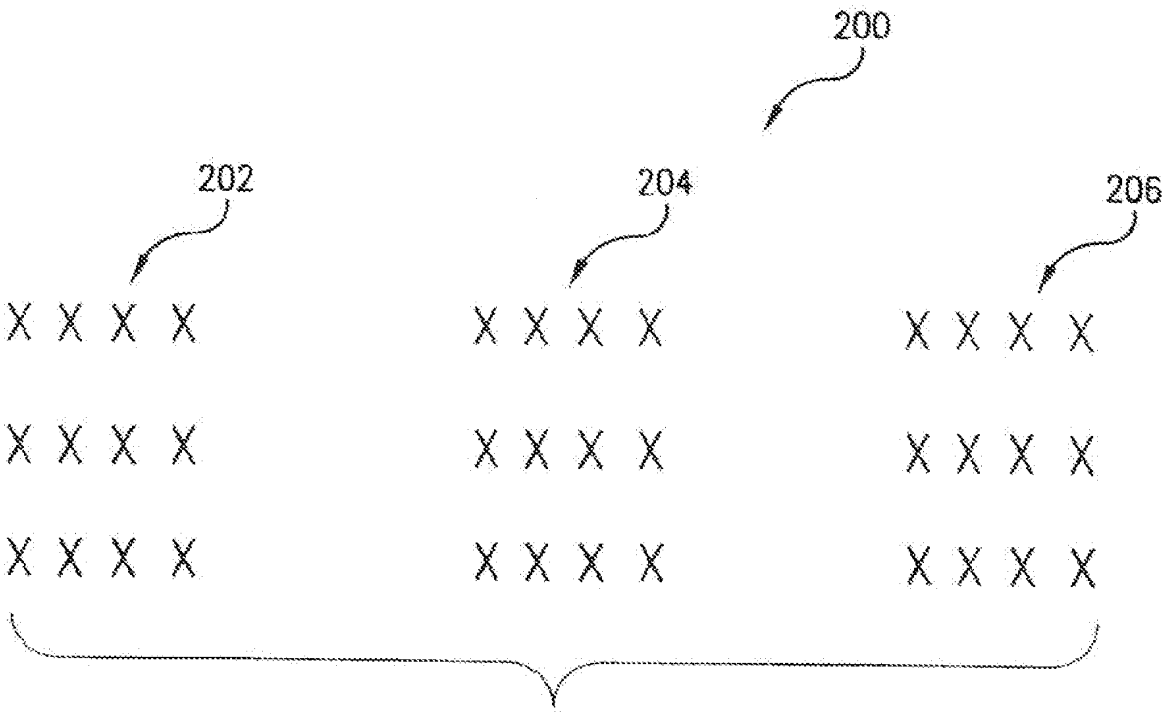


FIG.5

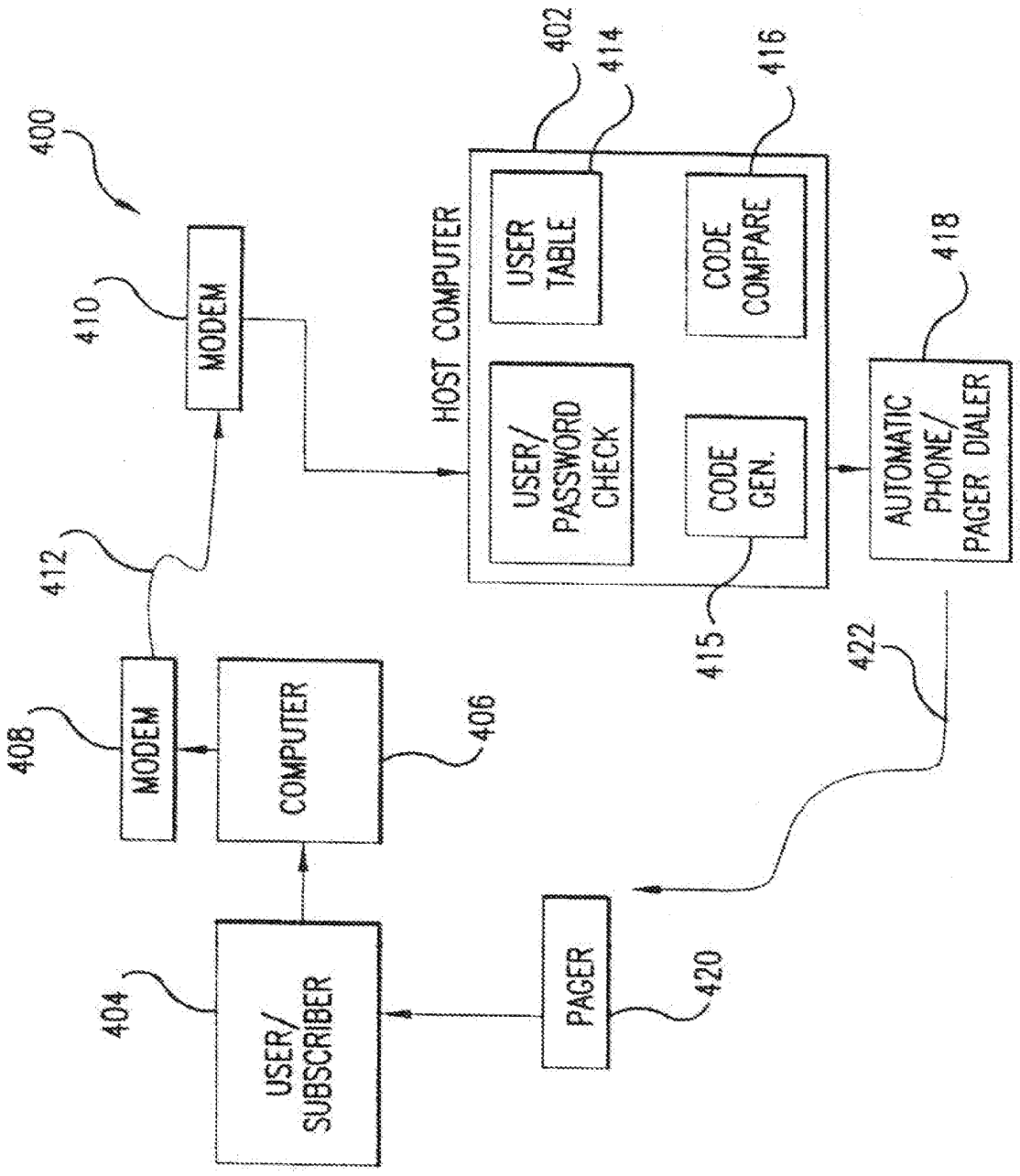

400
410
MODEM
412
408
MODEM
COMPUTER
406
404
USER/
SUBSCRIBER
PAGER
420
422
HOST COMPUTER
402
414
416
USER
TABLE
CODE
COMPARE
USER/
PASSWORD
CHECK
CODE
GEN.
415
418
AUTOMATIC
PHONE/
PAGER DIALER

FIG.6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 844 551 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.07.1998 Bulletin 1998/27

(43) Date of publication A2:
27.05.1998 Bulletin 1998/22

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **97890210.4**

(22) Date of filing: **22.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **28.10.1996 US 738897**

(71) Applicant: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(72) Inventor: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(74) Representative: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

(54) Computer security system

(57) Several embodiments of computer security systems are described and which are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream. In one embodiment, the security system comprises: an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel, analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to a code; and a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means; and a notification means for receiving said code and for notifying said authorized individual of the identity of said code.

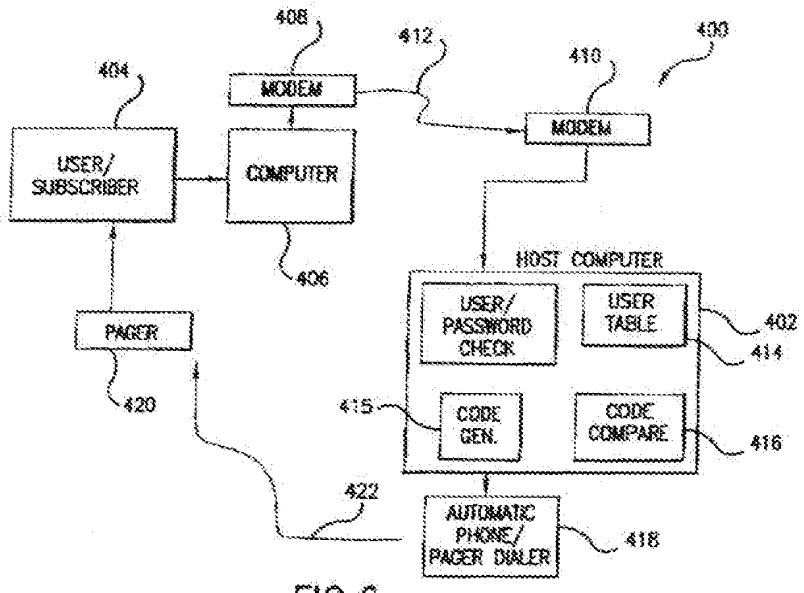


FIG.6

EP 0 844 551 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 89 0210

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 95 19593 A (KEW MICHAEL JEREMY ;LOVE JAMES SIMON (GB)) * abstract; figure 1 * * page 1, line 20 - page 3, line 23 *	1,5	G06F1/00
Y		6	
X	GB 2 229 020 A (ELLIS CHRIS KEIRON) * abstract * * page 3, paragraph 2 - page 6, last paragraph * * page 7, paragraph 2 - page 8, paragraph 1 *	2	
Y		6	
A	EP 0 558 326 A (HUGHES AIRCRAFT CO)		
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 February 1998	POWELL D.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

- ☐ All claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for all claims.
- ☐ Only part of the claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claims:
- ☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions.
namely:

See Sheet B.

- ☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.
- ☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:
- ☒ None of the further search fees has been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims: 1,2,5,6

BNSDOCID: <EP 0844551A3 >

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 97 89 0210

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1,2,5,6

   Secure access to a computer

2. Claim : 3

   Data transmission using plural channels

3. Claim : 4

   Data transmission with interspersed filler data

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 075 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.05.2003 Bulletin 2003/21

(51) Int Cl.7: **G07F 19/00**

(21) Application number: **02251152.1**

(22) Date of filing: **20.02.2002**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 JP 2001352947**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

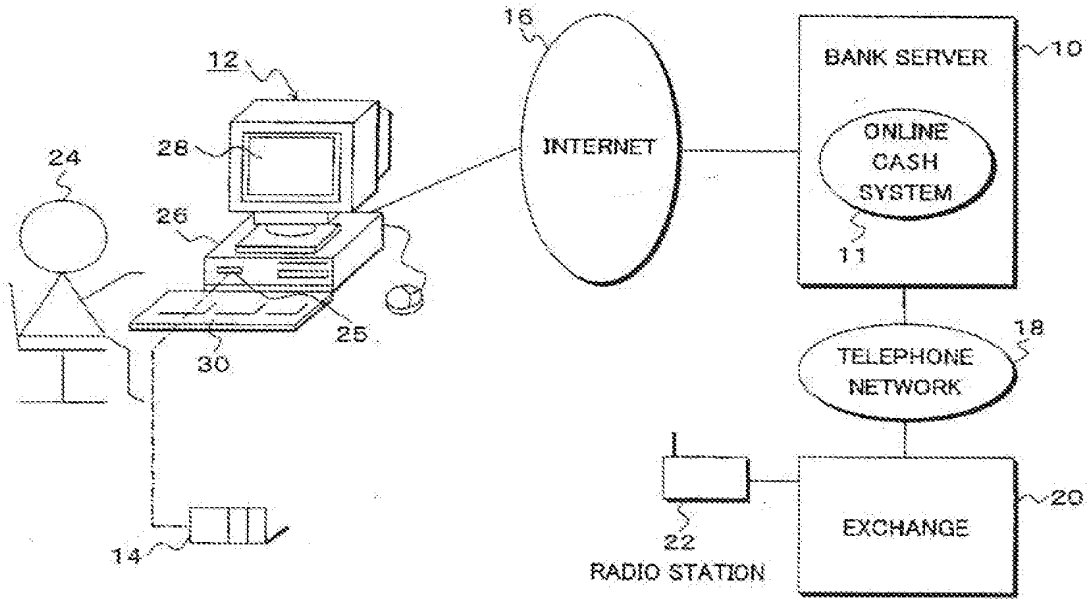
(72) Inventor: **Okamura, Michio, c/o Fujitsu Limited**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative: **Stebbing, Timothy Charles et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Electronic money processing method and program

(57) An electronic money system is constructed by: a terminal apparatus (12) of the user; an electronic money card (14) having an interface which can be connected to the terminal apparatus and a mobile phone function; and a bank server (10) which is connected to the terminal apparatus via the internet (16) and connected to the electronic money card (14) via a mobile telephone network. A payment request in which a payment money amount and a payment date/time have been designated is notified to the bank server (10) by the terminal apparatus (12). When the payment date/time arrives, a telephone call is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of electronic money to the card is executed. By setting a payment date/time in the future, payment to a lost or stolen card can be prevented.

FIG. 1



EP 1 313 075 A2

Description

[0001] The invention relates to an electronic money processing method for performing a card withdrawal of electronic money by an electronic money card, a terminal apparatus of the user, a bank server, a program for realizing such a method (which may be stored on a recording medium), and an electronic money system.

[0002] Hitherto, an electronic money card represented by a smart card has been used as a medium for performing shopping or the like by using electronic money in place of bills (banknotes) or coins.

[0003] In such an electronic money card, an IC chip built into the card has an MPU and a memory. By installing electronic money software in the memory, payment of electronic money can be made from a bank account into the card by using an ATM or the like of a bank, and payment for shopping or services can be made by debiting a balance of electronic money stored in the card.

[0004] However, in an electronic money system using such an electronic money card, to transfer funds from the bank account to the electronic money card, the electronic money card has to be set into the ATM or the like of the bank and operated in a manner similar to conventional cash withdrawal. Inconvenience still remains as compared with convenience of online banking using the Internet which can be used around the clock. To solve such a drawback, there has been considered an electronic money system incorporating a wireless communication function. For example, by building a PHS (Personal Handyphone System) function into the electronic money card, payment of electronic money from the bank account and payment to an electronic register or a vending machine can be made in an online manner by using a PHS telephone network. PHS is a cellular telephone system in use in Japan.

[0005] However, an electronic money card having a wireless communication function has a large problem in terms of security against illegal use due to theft or loss of the card, similar to that with an ordinary cellular phone. There is a great risk that electronic money is withdrawn from the bank account and used before the user becomes aware of the theft or loss of his card and takes a necessary procedure such as informing the bank which issued the card. Although the electronic money card can be provided with security functions such as a user-performed authenticating function, encrypting/decrypting function, mutual authenticating function, digital signature function, or an access control function on the assumption that the card is illegally used, the security is not always perfect against illegal use by a criminal act. Therefore there is still cause for concern in terms of the security.

[0006] According to the invention, an electronic money processing method is provided which assures high security against payment from a bank account in an online manner, by a relatively simple mechanism using an electronic money card having a wireless communication (e.g., mobile phone) function. A program for realizing such a method and a recording medium storing the program are also provided.

[0007] According to the invention, there is provided an electronic money processing method for a bank server which is connected to a terminal apparatus of the user via a communication network (which may be a fixed network such as the Internet), and connected via a wireless communication network to an electronic money card having an interface that can be connected to the terminal apparatus and a wireless communication function. The method comprises:

a payment accepting step wherein a payment application (payment request) in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated, is received from the terminal apparatus; and

a payment executing step wherein when the payment date/time is reached, a wireless communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money (i.e. transfer to the card) is executed.

[0008] According to another aspect of the invention, there is provided an electronic money processing method for a bank server, comprising:

a payment accepting step wherein a payment application in which a payment money amount has been designated, is received from the terminal apparatus; and

a payment executing step wherein a payment date/time is set by changing a time lag from a payment application date/time at which the payment application has been received in accordance with the accepted payment money amount, when the payment date/time arrives, a wireless communication is made to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed. In this case, the above processing method may further comprise the step of notifying the terminal apparatus of the set payment date/time.

[0009] As mentioned above, according to the invention, by providing the time lag between the payment application and the payment execution, even if loss or theft of the electronic money card occurs, by requesting the bank to stop the payment execution or requesting a network to prevent establishment of the wireless communication (i.e. stop the connection) prior to the set payment date/time, the execution of illegal withdrawal can be prevented. For example, the larger the payment money amount is, the larger the time lag between the

payment application date/time and the payment date/time is. Therefore, the larger the sum being transferred, the longer a time margin until any illegal withdrawal can be performed. During such an interval, a countermeasure for stopping execution of the payment can be certainly taken. Although a possibility exists that the security is broken and the payment application is made illegally since the payment application is made via the Internet, with respect to the actual execution of the payment, the network can be irrevocably requested to prevent the connection. Then, it is impossible to cancel such a request over the Internet or in any other way, so that high security is assured also with respect to this point.

[0010] In the payment applying step, real-time payment and a designation payment date/time may be prepared as a payment date/time and the user can be allowed to select either of them. In the payment applying step, the payment date/time in which the time lag between the payment application date/time and the payment execution date/time has been changed in accordance with the payment money amount inputted by the user can be also automatically set. In the payment applying step, prior to notifying the payment application, predetermined user authentication information including an account number and a telephone number (or network device identifier) obtained from the electronic money card may be transmitted from the terminal apparatus to the bank server, thereby obtaining authentication. Therefore, the user can easily access the bank server for the purpose of applying for the payment without needing to input the account number and the telephone number. The user authentication information includes a name, an address, and a personal identification number which were inputted by the user in addition to the account number and the telephone number obtained from the electronic money card. In the payment executing step, it may be determined that a phone number of an originator obtained by the communication from the bank server lies within a predetermined range (selection) of bank telephone numbers which have previously been stored, and an automatic response is made, thereby establishing a connection (telephone talk connection). In the payment executing step, if the connection is not established when the wireless communication is made from the bank server to the electronic money card, the execution of the payment is stopped and the payment application is cancelled. Such a situation corresponds to a case where a request to stop the connection has been made to the wireless network following loss or theft of the card. In addition, in the payment executing step, a payment stop can be inputted to the bank server prior to a payment term, thereby stopping the execution of the payment and cancelling the payment application. Such a situation corresponds to a case where the bank is requested to stop the payment following loss or theft of the card.

[0011] The invention provides a program which is executed by the bank server. The program allows a computer forming a bank server, which is connected to a terminal apparatus of the user via a communication network such as the Internet and connected via a wireless communication network to an electronic money card having an interface that can be connected to the terminal apparatus and a wireless communication function, to execute:

a payment accepting step wherein a payment application (transfer request), in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated, is received from the terminal apparatus; and
a payment executing step wherein when the payment date/time is reached, a wireless communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed. Thus, the card is replenished.

[0012] According to another aspect of the invention there is provided a program which is executed by a bank server, the program allowing a computer forming the bank server to execute:

a payment accepting step wherein a payment application in which a payment money amount has been designated is received from the terminal apparatus; and
a payment executing step wherein a payment date/time is set by changing a time lag from a payment application date/time at which the payment application has been received in accordance with the accepted payment money amount, when the payment date/time arrives, communication is made to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money to the card is executed.

[0013] The invention also provides a computer-readable recording medium in which a program which is executed by a bank server has been stored. The recording medium stores the program for allowing a computer forming a bank server which is connected to a terminal apparatus of the user via a communication network such as the Internet and connected via a wireless communication network to an electronic money card having an interface that can be connected to the terminal apparatus and a wireless communication function, to execute:

a payment accepting step wherein a payment application, in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have

been designated, is received from the terminal apparatus; and

a payment executing step wherein when the payment date/time comes, communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0014] According to another aspect of the invention, there is provided a recording medium in which a program which is executed by a bank server has been stored, the program allowing a computer forming the bank server to execute:

a payment accepting step wherein a payment application, in which a payment money amount has been designated, is received from the terminal apparatus; and

a payment executing step wherein a time lag from a payment application date/time at which the payment application has been received is changed in accordance with the accepted payment money amount, a payment date/time is set, when the payment date/time comes, communication is made to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0015] The invention provides an electronic money processing method for a terminal apparatus in which an electronic money card having an interface and a wireless communication function is connected to a card interface (e.g. a physical slot) and which is connected, e. g. via the Internet, to a bank server that is connected to the electronic money card via a communication network. The electronic money processing method for the terminal apparatus comprises:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number (device identifier) obtained from the electronic money card is transmitted from the terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein the bank server is notified of a payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated,

wherein at the payment date/time, communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0016] According to another aspect of the invention, there is provided an electronic money processing method for a terminal apparatus, comprising:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from the electronic money card is transmitted from the terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein the bank server is notified of a payment application in which a payment money amount has been designated,

wherein at a payment date/time which has been set by changing a time lag from a payment application date/time at which the payment application is received in accordance with the payment money amount accepted by the bank server, a communication channel is opened to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed. Details in this case are fundamentally the same as those in case of the processing method of an electronic money system.

[0017] The invention provides a program for a terminal apparatus. The program allows a computer, forming a terminal apparatus in which an electronic money card having an interface and a communication function is connected to a card interface and which is connected e. g. via the Internet to a bank server that is connected to the electronic money card via a communication network, to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from the electronic money card is transmitted from the terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein the bank server is notified of a payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated,

wherein when the payment date/time is reached, a communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and the payment applied for is made to the card.

[0018] According to another aspect of the invention of a program for a terminal apparatus, the program allows a computer forming the terminal apparatus to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from an electronic money card is transmitted from the terminal apparatus to a bank server and authentication is obtained; and

a payment applying step wherein the bank server

is notified of a payment application in which a payment money amount has been designated,

wherein at a payment date/time which has been set by changing a time lag from a payment application date/time at which the payment application is received in accordance with the payment money amount accepted by the bank server, communication is made to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed. Details in this case are fundamentally the same as those in case of the processing method of an electronic money system.

[0019] The invention further provides a computer-readable recording medium in which a program for a terminal apparatus has been stored. The recording medium stores the program for allowing a computer forming the terminal apparatus in a system in which an electronic money card having an interface and a communication function is connected to a card interface and which is connected to a bank server that is connected to the electronic money card via a communication network, to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from the electronic money card is transmitted from the terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein the bank server is notified of a payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated,

wherein when the payment date/time arrives, communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0020] According to another aspect of the invention there is provided a recording medium in which a program for a terminal apparatus has been stored, the program allowing a computer forming the terminal apparatus to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from an electronic money card is transmitted from the terminal apparatus to a bank server and authentication is obtained; and

a payment applying step wherein the bank server is notified of a payment application in which a payment money amount has been designated,

wherein at a payment date/time which has been set by changing a time lag from a payment application date/time at which the payment application is received in accordance with the payment money amount accepted by the bank server, communication is made to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed. Details in this case are fundamentally the same as those in case of the processing method of an electronic money system.

[0021] The invention provides a processing method for an electronic money card which is coupled to a terminal apparatus of the user e.g. by insertion into a slot, and connected to a bank server via a wireless communication network. The processing method for the electronic money card comprises:

a payment supporting step wherein when a payment application in which at least a payment money amount has been designated is notified to the bank server by the terminal apparatus, the user's own telephone number (or card network address) and account number which have previously been stored are provided; and

a payment receiving step wherein at a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount, if a communication is received from the bank server, establishment of a connection is confirmed, and payment of the electronic money is received by the card.

[0022] The invention provides a program for an electronic money card. The program allows a computer built in the electronic money card which is connected to a terminal apparatus of the user and connected to a bank server via a wireless communication network to execute:

a payment supporting step wherein when a payment application in which at least a payment money amount has been designated is notified to the bank server by the terminal apparatus, the user's own telephone number and account number which have previously been stored are provided; and

a payment receiving step wherein at a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount, if a communication is received from the bank server, establishment of a connection is confirmed, and payment of the electronic money is received.

[0023] The invention also embraces a computer-readable recording medium in which a program for an electronic money card has been stored. The program stored in the recording medium allows a computer built in the electronic money card which is connected to a

terminal apparatus of the user and connected to a bank server via a communication network to execute:

a payment supporting step wherein when a payment application in which at least a payment money amount has been designated is notified to the bank server by the terminal apparatus, the user's own telephone number and account number which have previously been stored are provided; and
a payment receiving step wherein when a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount comes, if a communication is received from the bank server, establishment of a connection is confirmed, and payment of the electronic money is received.

[0024] The invention provides an electronic money system. The electronic money system comprises: a terminal apparatus of the user; an electronic money card having an interface which can be connected to the terminal apparatus and a wireless communication function; and a bank server which is connected to the terminal apparatus e.g. via the Internet and connected to the electronic money card via a wireless communication network, wherein a payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with the payment money amount have been designated is notified to the bank server from the terminal apparatus, when the payment date/time comes, communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0025] According to another aspect of an electronic money system of the invention, the system comprises: a terminal apparatus of the user; an electronic money card having an interface which can be connected to the terminal apparatus and a wireless communication function; and a bank server which is connected to the terminal apparatus e.g. via the Internet and connected to the electronic money card via a wireless network,
wherein a payment application in which a payment money amount has been designated is notified to the bank server from the terminal apparatus, a payment date/time is set by changing a time lag from a payment application date/time in accordance with the payment money amount accepted by the bank server, when the set payment date/time comes, communication is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of the electronic money is executed.

[0026] Reference will now be made, by way of example only, to the accompanying drawings in which:

Fig. 1 is an explanatory diagram of a bank online cash system to which the invention is applied;
Fig. 2 is an external explanatory view of an electronic money card which is used in the invention;
Fig. 3 is a block diagram showing an internal construction of the electronic money card in Fig. 2;
Fig. 4 is an explanatory diagram of a memory area in Fig. 3;
Figs. 5A and 5B are block diagrams showing a functional construction of the invention corresponding to the system of Fig. 1;
Figs. 6A to 6C are time charts for a processing procedure for electronic money payment according to the invention;
Figs. 7A and 7B are flowcharts for an electronic money processing program of the invention which is executed by a bank server;
Figs. 8A and 8B are flowcharts for an electronic money processing program of the invention which is executed by a terminal apparatus; and
Figs. 9A and 9B are flowcharts for a processing program of the invention which is executed by the electronic money card.

[0027] In the following, a preferred embodiment of the invention will be described with reference to a Personal Handyphone System (PHS) as an example. However, the invention is not limited to use with PHS and may employ any wireless communication system capable of exchanging messages, such as GSM, pager networks etc. Further, the invention need not employ a primary voice channel within such a system, but may instead employ a signalling channel provided in the system. In addition, a combination of a fixed-line and wireless networks (including short-range wireless networks) may be used.

[0028] Fig. 1 is a system constructional diagram of a bank online cash system to which a processing method for an electronic money system of the invention is applied. A bank server 10 is provided with an online cash system 11 having the electronic money system of the invention. A terminal apparatus 12 of a user 24 is connected as a client to the bank server 10 via an Internet 16. The terminal apparatus 12 is a personal computer or the like and comprises a main body 26, a display unit 28 such as a color display, and an operation unit 30 having a keyboard, a mouse, and the like. Further, the main body 26 has a card slot 25 into which a card is inserted and connected via a PCMCIA interface. The user 24 has a PHS electronic money card 14 in order to use the online cash system 11 of the bank server 10. Electronic money processing software has been installed as ROM software into the PHS electronic money card 14. The PHS electronic money card 14 has a PHS (simple Personal Handyphone System) function and a PCMCIA (Personal Computer Memory Card International Association) interface which is inserted and connected into the card slot 25 of the terminal apparatus 12 in order to input and output data to/from an outside. The bank server 10 is connected to a PHS telephone network in order to execute input/output processes via the PHS function

of the PHS electronic money card 14. The PHS telephone network is constructed by a telephone network 18, an exchange 20, and a radio station 22. According to the processing method for the electronic money system of the invention, in a state where the user 24 has inserted and connected the PHS electronic money card 14 into the card slot 25 of the terminal apparatus 12, the user accesses a homepage of the bank server 10 via the Internet 16. After user authentication is obtained by using a screen of the homepage downloaded from the bank server 10, the terminal apparatus is subjected to switching by a download of a withdrawal screen. A request for payment from a bank account to the PHS electronic money card 14 is made to the online cash system 11 of the bank server 10 via the Internet 16. A feature of the payment request in the processing method for the electronic money system of the invention is as follows. Payment application in which a payment money amount and a payment date/time have been designated is made from the terminal apparatus 12 to the bank server 10. In the bank server 10 which accepts the payment application, when a payment term designated by the user 24 comes, the PHS electronic money card 14 is directly called by the PHS telephone network, payment is executed after waiting for an automatic response. Therefore, a time lag exists in a time interval from the payment application by the user to the payment execution from the bank server 10 to the PHS electronic money card 14. Security against loss or theft of the PHS electronic money card 14 is assured by such a time lag.

[0029] Fig. 2 is an external explanatory view of the PHS electronic money card in Fig. 1. The PHS electronic money card 14 has an antenna 32, at one end, which is used for radio transmission of the PHS telephone network and PHS transceiver transmission of an electronic register, an automatic vending machine, an automatic ticket gate, or the like. An information display apparatus 34 and a button apparatus 36 are provided on the card surface. The information display apparatus 34 uses a display such as an LCD or the like of a low electric power consumption type. In a normal mode, a PHS phone number and a present balance of electronic money are displayed as shown in the diagram. The button apparatus 36 transmits its own PHS phone number to a partner apparatus such as electronic register, automatic vending machine, automatic ticket gate, or the like and activates an access by using a built-in PHS transceiver function. At this time, a situation of the transmission and reception of the electronic money is displayed on the information display apparatus 34. A PCMCIA interface 38 is provided on the reverse side of the card. By inserting the portion of the PCMCIA interface 38 into the card slot 25 of the terminal apparatus 12 in Fig. 2, information can be transmitted and received to/from the PHS electronic money card 14.

[0030] Fig. 3 is a block diagram showing a hardware construction of the PHS electronic money card 14. A PHS communication control apparatus 40 and a PHS telephone communication apparatus 42 are provided for the PHS electronic money card 14 in order to make PHS communication. Information can be transmitted and received to/from the PHS telephone network by a telephone talk connection by using the antenna 32. A PHS transceiver apparatus 44 is provided for the PHS communication control apparatus 40. By the PHS transceiver apparatus 44, information is transmitted and received to/from the partner apparatus such as electronic register, automatic vending machine, automatic ticket gate, or the like serving as a payment destination of the electronic money. A processing function of the PHS electronic money card 14 is realized by PHS electronic money processing software 46. Specifically speaking, the portion of the PHS electronic money processing software 46 is a portion where the program is executed by an MPU. Actually, a set of software for processing electronic money information has been stored in an ROM memory 48. By executing necessary software on the MPU, the function of the PHS electronic money processing software 46 is realized. Information regarding the electronic money has been stored in a memory 50. A DRAM is used as a memory 50. Further, PCMCIA interface software 52 is provided. In a state where it has been inserted and connected into the card slot 25 of the terminal apparatus 12 as shown in Fig. 2, necessary information can be transmitted and received between the PHS electronic money processing software 46 and the electronic money processing software on the terminal apparatus side.

[0031] Fig. 4 is an explanatory diagram of management information in the memory 50 provided for the PHS electronic money card 14 in Fig. 3. An area of the memory 50 is constructed by an electronic money information area 74, a credit information area 76, a periodic information area 78, a household accounts information area 80, and further, an ROM software work area 82. As information necessary for the processing method for the electronic money system of the invention, a bank account number and a PHS phone number of the user and, further, the electronic money balance have been stored in the electronic money information area 74. Sex and birthday have been stored as attribute information of the user in the electronic money information area 74. Further, in order to write boarding start information at the time of boarding to a train, a bus, a freeway, or the like and pay a charge at the time of alighting by electronic money, the boarding start information can be stored into the electronic money information area 74. A company code for identifying a credit company, a credit number, and a validity term are stored in the credit information area 76. The following detailed information is, for example, stored into the periodic information area 78: that is, a code of a company which pays for a charge for a commutation ticket or a coupon ticket; a code of a vehicle kind such as train, bus, automobile, taxi, airplane, or the like; a purchase kind code for identifying whether a ticket is a commutation ticket, a coupon ticket, or a passenger

ticket; information of a boarding period of the commutation ticket or coupon ticket; information of a boarding interval of the commutation ticket or coupon ticket; a degree of purchase of the coupon ticket; purchaser's discount information; and the like The following information is stored into the household accounts information area 80: that is, a division showing a kind of payment or reception; a date/time; a kind indicative of an electronic money withdrawal from an ATM, an electronic money withdrawal in an online manner, a charge payment of a PHS electronic money card, an internet payment by the PHS electronic money card, or the like; a telephone number on the partner PHS electronic money side who paid the charge; money amount information showing whether the charge is a payment charge or a withdrawal charge; shop information of a shop in which the charge was paid by the electronic money; article information of the article paid by the electronic money; his own personal identification number of the user who uses an Internet online shop; a personal identification number of the partner side who uses an Internet online shop; a payment completion display which is turned on in the case where a charge payment notification is received from a payment destination partner and the charge is paid in case of the kind indicative of the Internet payment by PHS electronic money (PHS-ON); and the like. Naturally, an information area regarding another electronic money use is provided into the memory 50 within an available range of a memory capacity as necessary.

[0032] Figs. 5A and 5B are block diagrams of a functional construction of each of the bank server, terminal apparatus, and PHS electronic money card in the processing method for the electronic money system according to the invention corresponding to the system construction of Fig. 1. Functions as a bank server electronic money processing unit 10-1 of the invention are provided for the online cash system 11 provided for the bank server 10 in Fig. 1. Functions as a terminal electronic money processing unit 12-1 are provided for the terminal apparatus 12 of the user. Further, functions as a card electronic money processing unit 14-1 are provided for the PHS electronic money card 14. The functions of the card electronic money processing unit 14-1 construct a part of the PHS electronic money processing software 46 shown in Fig. 3. A customer recording database 54 is provided for the bank server electronic money processing unit 10-1. A user account number, a name, an address, a personal identification number, and an electronic money card telephone number have been stored every use customer into the customer recording database 54. In order to accept payment application of the user and execute payment to the PHS electronic money card 14, functions of a payment authenticating unit 56, a payment accepting unit 58, and a payment executing unit 60 are provided for the bank server electronic money processing unit 10-1. An authentication obtaining unit 62 and a payment applying unit 64 are provided for the terminal electronic money processing unit 12-1 in the terminal apparatus 12 of the user. When the payment is applied for to the bank server 10 by using the terminal electronic money processing unit 12-1, the PHS electronic money card 14 is inserted and connected into the card slot 25 of the terminal apparatus 12 as shown in Fig. 1. In this state, the card electronic money processing unit 14-1 is connected to the terminal electronic money processing unit 12-1 via the PCMCIA interface 38 as shown in Fig. 6. Further, the terminal electronic money processing unit 12-1 is connected to the bank server electronic money processing unit 10-1 via the Internet 16. The card electronic money processing unit 14-1 is connected to the bank server electronic money processing unit 10-1 via a PHS telephone network 72. A paying process by the online cashing in the processing method for the electronic money system in the invention is mainly classified into the following two processes.

(1) Payment application
(2) Payment execution

A time lag is purposely provided between those two processes. The authentication obtaining unit 62 and payment applying unit 64 provided for the terminal electronic money processing unit 12-1 make the payment application for the PHS electronic money card 14 to the bank server 10 side. Prior to the payment application, the authentication obtaining unit 62 first obtains authentication for the payment application from the bank server electronic money processing unit 10-1. Specifically speaking, when the homepage of the bank server 10 is accessed from the terminal apparatus 12 and the item of the payment is selected from a menu screen, the screen is switched to an authentication obtaining screen. By using the authentication obtaining screen, the user sets the address, name, and personal identification number as shown in the authentication obtaining unit 62. Although the account number and the PHS phone number are necessary upon obtaining of the authentication, the authentication is automatically obtained by accessing a payment supporting unit 68 via the PCMCIA interface 38 from the card electronic money processing unit 14-1 on the PHS electronic money card 14 side connected to the card slot 25. Therefore, with respect to the setting of the user authentication information upon obtaining of the authentication, the user does not need to input and set the account number and the PHS phone number and they can be automatically inputted and set from the card side. If the user authentication information could be set as mentioned above, the user makes an authenticating request to the bank server electronic money processing unit 10-1 via the Internet 16. In response to the authenticating request, the corresponding user account number, name, address, personal identification number, and electronic money card telephone number are obtained from the user authentication information received by the payment au-

thenticating unit 56 and the customer recording database 54, thereby collating the user. When coincidence is obtained as a result of the collation, a payment application screen is downloaded to the terminal electronic money processing unit 12-1, thereby allowing the unit 12-1 to switch the screen. By the download from the server 10 side, the screen on the terminal apparatus 12 side is switched to the screen for payment application. The function of the payment applying unit 64 in the terminal electronic money processing unit 12-1 is constructed. Therefore, the user sets two items "payment money amount" and "payment date/time" by using the switched screen for payment. Upon setting of the payment application information in the invention, although the user inputs and sets the "payment money amount" as necessary, either a "real-time payment" or a "payment date/time" by the user setting can be selected with respect to the "payment date/time". In the normal payment application, the payment date/time by the setting input of the user is set. However, in case of urgency, the real-time payment can be selected. In the real-time payment, as for the time lag which is caused between the payment application and the payment execution, the execution of the payment to the PHS electronic money card 14 is completed within the minimum time which is determined by a communicating process for application by the Internet 16, a processing time on the server side, and a transmitting time by the PHS telephone network 72. The payment date/time can be also changed by the function of the payment applying unit 64 in accordance with the payment money amount set by the user. For example, if the payment money amount is less than 50,000 yen, the real-time payment is also enabled to be selected. If the payment money amount lies within a range between 50,000 yen and an amount less than 100,000 yen, the time lag is set to 3 days. If the payment money amount is equal to or larger than 100,000 yen, the time lag is set to 5 days. In this manner, the payment date/time is set in a manner such that as the payment money amount is larger, the time lag between the payment application date/time and the payment execution date/time is increased. Thus, the time lag between the payment application and the payment execution is extended when the payment money amount is large, thereby certainly assuring the security in the case where loss or theft of the PHS electronic money card 14 occurred for the time interval from the payment application to the payment execution. The payment information of the payment money amount and payment date/time set by the user is transmitted to the bank server electronic money processing unit 10-1 via the Internet 16 and processed by the payment accepting unit 58. The payment accepting unit 58 recognizes the payment money amount from the received payment application information, recognizes the payment date/time, and subsequently activates a monitoring process until the date/time reaches the designated payment date/time. When the payment applying operation as mentioned above is finished, the user removes the PHS electronic money card 14 from the terminal apparatus 12. When the user goes out or the like, he carries the PHS electronic money card 14 and makes payment by the electronic money by using the built-in transceiver function in case of the payment for purchase, the payment at a ticket gate of transport facilities, or the like. In the bank server electronic money processing unit 10-1, when the date/time reaches the payment date/time set by the application acceptance in the payment accepting unit 58, the payment executing unit 60 is activated, thereby executing the payment by accessing the card electronic money processing unit 14-1 of the PHS electronic money card 14 by using the PHS telephone network 72. Upon execution of the payment, the PHS electronic money card 14 is directly called via the PHS telephone network 72 by the originating operation based on the electronic money card phone number recognized by the payment application. In response to such a call from the bank server 10 side, a payment receiving unit 68 of the card electronic money processing unit 14-1 automatically responds. The automatic response by the payment receiving unit 68 is made under the following conditions. That is, the telephone number of the originator is compared with bank phone number range information which has previously been written in the memory 50 of the PHS electronic money card 14. If the telephone number of the originator lies within the bank phone number range, it is determined that the telephone call is a call from the bank server electronic money processing unit 10-1, and an incoming response is automatically started. As with bank phone number range information which is used for discriminating the call from the bank server 10, for example, two kinds of numbers of a lower limit (11 digits) of a bank phone number band and an upper limit (11 digits) of a bank phone number band are written into the ROM memory 48 of the PHS electronic money card 14. If the telephone number of the originator lies within a range between the lower limit bank phone number band and the upper limit bank phone number band, it is decided that the telephone call is a call from the correct bank server, and an incoming response is automatically started. If the incoming response is obtained by the calling to the PHS electronic money card 14, since a telephone talk connection via the PHS telephone network 72 is established, the payment executing unit 60 transmits the electronic money payment information by using this connecting state. The electronic money payment information includes the payment money amount, time information, and bank name. The payment receiving unit 68 of the card electronic money processing unit 14-1 which received the payment information from the bank server 10 side updates an electronic money balance by adding the received payment money amount to a present electronic money balance and, further, stores the time information and the payment information such as a bank name and the like. If the PHS electronic money card 14 is lost or stolen after the payment application

was made from the terminal apparatus 12 to the bank server 10, a procedure to stop the payment execution is taken. The procedure to stop the payment execution includes, for example, the following two steps.

(1) The user contacts a main bank having the payment account of the PHS electronic money card and requests the payment stop because of the loss or theft.
(2) The user contacts a telephone company of the PHS telephone network and requests the telephone talk stop of the PHS telephone because of the loss or theft.

[0033] If the main bank receives the payment stop notice from the user, by executing the payment stopping operation with respect to the relevant account number, the payment execution by the monitoring of the payment term set by the acceptance of the application made by the payment accepting unit 58 of the bank server electronic money processing unit 10-1 is cancelled. Therefore, even if the payment date/time comes, payment is not performed from the bank server 10 side to the lost or stolen PHS electronic money card 14. By setting the time lag between the payment application date/time and the payment execution date/time so as to be longer in accordance with the payment money amount, a time margin in which the procedure to stop the payment execution can be taken is extended in accordance with the money amount.

[0034] When the stop of the PHS telephone is applied, even if the payment accepting unit 58 in the bank server electronic money processing unit 10-1 activates the payment executing unit 60 when the accepted payment date/time comes and the originating operation is performed to the PHS electronic money card 14 by the PHS telephone network 72, since the procedure for stopping the telephone talk has already been taken in its exchange, a telephone talk connection to the PHS electronic money card 14 by the PHS telephone network 72 cannot be established. The payment to the lost or stolen PHS electronic money card 14 is not executed.

[0035] Figs. 6A to 6C are time charts showing a procedure in a range between the payment application and the payment execution in the electronic money system of the invention with respect to the processes and transmission/reception which are executed among the bank server 10, terminal apparatus 12, and PHS electronic money card 14. In Fig. 6A, first, the terminal apparatus 12 accesses the home page of the bank server 10 via the internet 16 in step S1. In response to it, the bank server 10 downloads the homepage in step S101, a menu screen for performing transaction of the online cash system is displayed in the terminal apparatus 12. Therefore, when the user selects "payment" from the menu screen, the screen is switched to an "authentication screen". In step S2, the user authentication information is set onto the authentication screen and an authenticating request is made to the bank server 10. At this time, the PHS electronic money card 14 has been inserted and connected to the card slot 25 of the terminal apparatus 12. The account number and PHS phone number in the user authentication information are automatically provided in response to the access from the terminal apparatus 12 in step S201. The bank server 10 which received the user authentication information from the terminal apparatus 12 collates the received user authentication information with the database in step S102. If the coincidence is obtained as a result of the collation in step S103, step S104 follows. The screen is switched to the payment screen, it is downloaded, and the payment screen is displayed on the terminal apparatus 12 side. If the coincidence as a collation result of the user authentication information is not obtained in step S103, the illegal use is determined and the bank server 10 finishes the process. In the terminal apparatus 12 which received the download and in which the screen has been switched to the payment screen, in step S3, the payment money amount and the payment date/time are set onto the switched payment screen and the payment application is made. When the payment date/time is set, duration of the time lag in the interval from the payment application date/time to the payment execution date/time in which the processes in steps S2 and S3 are executed is changed in accordance with the money amount. When the payment application from the terminal apparatus 12 is received, the bank server 10 starts to monitor the accepted payment date/time in step S105. Subsequently, in Figs. 6B and 6C, whether a payment stop instruction has been issued or not is discriminated in step S106. If NO, whether the payment date/time has come or not is discriminated in step S108. The checking processes in steps S106 and S108 are repeated. If the PHS electronic money card 14 is lost or stolen after the payment was applied for, the user requests the main bank to stop the payment, so that it is determined that the payment stop has been instructed in step S106. In this case, step S107 follows, a payment stopping process is executed, and the payment execution is cancelled. If it is decided in step S108 that whether the payment date/time has come, the bank server 10 makes a telephone call of the PHS electronic money card 14 in step S109. In step S202, the PHS electronic money card 14 which received the telephone call compares the phone number of the originator with the bank telephone number range which has previously been held. If it lies within the range, an automatic incoming response is made, so that the telephone talk connection is established. When the bank server 10 confirms the incoming response from the card 14 side in step S110, step S112 follows and the payment money amount, time, bank name, and the like are transmitted as bank money payment information. If the PHS electronic money card 14 is lost or stolen after the payment was applied for and the user has already applied for the stop of the telephone talk to the PHS telephone company, a counter-

measure for stopping the telephone talk is taken in the PHS telephone network in response to the telephone call to the lost or stolen PHS electronic money card 14 in step S109. If the telephone talk connection with the card 14 side is not established and it is determined that there is no telephone talk response in step S110, step S111 follows and the bank server 10 cancels the payment execution. If the electronic money payment information is normally transmitted in step S112, the PHS electronic money card 14 updates the electronic money balance by adding the payment money amount obtained from the received electronic money payment information to the present electronic money balance and further stores the time and the bank name. In step S204, a normality end is notified and the telephone talk connection is disconnected. When the normality end notice from the card side is received, the bank server 10 executes a payment finishing process in step S113.

[0036] Figs. 7A and 7B are flowcharts for an electronic money processing program which is executed by the bank server 10. In Fig. 7A, the bank server 10 checks a user access in step S1. When there is a user access, the homepage is downloaded in step S2. Subsequently, in step S3, the bank server 10 discriminates whether the user authentication information has been received or not. If the user authentication information is received, it is collated with the database in step S4. If a coincidence is obtained as a collation result in step S5, the screen is switched to the payment screen and the payment screen is downloaded in step S6. If the coincidence is not obtained, the processing routine is finished. In step S7, whether the payment application has been received or not is discriminated. If it is received, the payment application is accepted and the monitoring of the payment date/time is started in step S8. Subsequently, the presence or absence of the payment stop instruction is discriminated in step S9 in Fig. 7B. If there is no stop instruction, whether the payment term has come or not is discriminated in step S11. If the payment stop instruction was issued before the payment term comes, the payment is cancelled in step S10. If the payment date/time comes, a telephone call of the PHS electronic money card 14 is made in step S12. If there is the incoming response in step S13, electronic money payment information such as payment money amount, time, bank name, and the like is transmitted in step S15. If there is no incoming response in step S13, the payment is cancelled in step S14. Upon discrimination in the case where there is no incoming response in step S13, when there is no incoming response in case of the telephone talk stop due to the loss, theft, or the like, the payment is immediately cancelled in step S14. However, in the case where the user does not exist in a communication area of the PHS telephone network, the telephone call in step S12 is made the predetermined number of times every elapse of a predetermined time. If the incoming response is not obtained even after the telephone call was made the predetermined number of times, the payment is cancelled in step S14. After the electronic money payment information is normally transmitted in step S15, the system waits for the reception of a normality end response from the card side in step S16. If the normality end response is received, the paying process is finished in step S17. If there is no normality end response in step S16, an abnormality finishing process is executed in step S18. In the abnormality finishing process, abnormality contents are recorded and the fact that the payment was cancelled is recorded.

[0037] Figs. 8A and 8B are flowcharts for the electronic money processing program of the invention which is executed in the terminal apparatus 12. When the payment is received to the PHS electronic money card 14, the terminal apparatus 12 accesses the homepage of the bank in step S1 in a state where the card has been inserted and connected into the card slot 25 of the terminal apparatus 12, and selects "payment" in step S2 from a menu screen thus obtained. Since the screen is switched to an authentication screen by the selection of the payment, the user authentication information is set into the authentication screen in step S3. At this time, whether the card has been connected or not is discriminated in step S4. If the card has been connected, the account number and the PHS phone number are obtained from the PHS electronic money card 14 in step S6. If the card is not connected, a message for card insertion is displayed in step S5, thereby urging the user to insert the card. Therefore, the system uses a mechanism such that unless the PHS electronic money card 14 is inserted and connected to the terminal apparatus 12, the payment from the bank account to the card cannot be applied for. Naturally, as another embodiment, it is also possible to use a mechanism such that even if the card is not inserted, the account number and the PHS phone number are set and inputted on the authentication screen by the setting/inputting operation of the user, thereby applying for the payment. If the account number and the PHS phone number can be obtained from the card 14 side in step S6, the user authentication information is transmitted to the bank server 10 in step S7. When the authentication is received from the bank server 10 in step S8, the screen is switched to the downloaded payment screen and displayed on the basis of the obtained authentication in step S9. In step S10, the payment money amount and the payment date/time are set into the payment screen and the payment is applied for to the bank server 10. A series of payment applying processes is finished. Naturally, if the authentication is not received from the bank server 10 in step S8, the processing routine is finished.

[0038] Figs. 9A and 9B are flowcharts for a processing program of the invention which is executed by the PHS electronic money card 14. In the PHS electronic money card 14, whether there is a read access from the terminal apparatus 12 or not is discriminated in step S1. If there is the read access, a response of the account number and the PHS phone number is made in step S2.

In step S3, whether there is a PHS telephone call from the bank server 10 or not is discriminated. If there is the telephone call, in step S4, the phone number of the originator is compared with the bank telephone number range which has previously been stored. If it is determined in step S5 that the phone number of the originator lies within the range as a result of the comparison, an automatic incoming response is made in step S6. Subsequently, in step S7, whether the payment information has been received from the bank server 10 or not is discriminated. If it is received, the electronic money balance is updated by adding the payment money amount to the present electronic money balance and, thereafter, the time and the bank name are stored in step S8. The bank server is notified of the normality end in step S9 and the telephone talk connection is subsequently disconnected in step S10. If the phone number of the originator is out of the bank telephone number range in step S5 or if the payment information is not received from the bank server side in step S7, the telephone talk connection is disconnected in step S10.

[0039] The invention provides a recording medium in which the program for the electronic money process in each of the bank server 10, terminal apparatus 12, and PHS electronic money card 14 has been recorded. An embodiment of the computer-readable recording medium in which each of the processing programs has been stored will be explained hereinbelow. Each of the processing programs has been recorded in a portable recording medium such as CD-ROM, floppy disk (R), DVD disk, magnetooptic disk, IC card, or the like, a database connected via a telephone line by using a modem, an LAN interface, or the like, or a database of another computer system. Each of the processing programs is installed into the bank server 10, terminal apparatus 12, and PHS electronic money card 14 having the functions as a computer and, thereafter, executed. Besides the portable recording medium such as CD-ROM, floppy disk (R), DVD disk, magnetooptic disk, IC card, or the like, the recording medium incorporates a storage device such as hard disk, memory, or the like provided in/out of the computer, a database for holding the programs via the line, another computer, its database, and further, a transmission medium on the line.

[0040] As another embodiment of the invention, with respect to the time lag between the payment application date/time and the payment execution date/time, only the payment money amount is transmitted from the payment applying unit 64 of the terminal apparatus 12 to the bank server 10. The payment accepting unit 58 which received the data of the payment money amount determines the payment execution date/time on the basis of the time lag according to the money amount and returns it to the terminal apparatus 12. In this case, it is also possible to construct the system in a manner such that the payment executing unit 60 of the bank server 10 makes a decision on the payment execution date/time based on the time lag according to the money amount and the payment accepting unit 58 returns the decided payment execution date/time to the terminal apparatus 12.

[0041] As mentioned above, according to the invention, by providing the time lag between the payment application (transfer request) and the payment execution (actual transfer of funds to the card), even if the electronic money card is lost or stolen, by requesting the bank to stop the payment or requesting the communication network to stop the connection prior to the payment date/time, the execution of the payment to the lost or stolen electronic money card can be certainly prevented, and the security of the bank online cash system using the electronic money card can be remarkably improved.

[0042] If the payment request is made via the Internet, a possibility remains that the payment application is made illegally. However, upon execution of the payment, by requesting the communication network to stop the connection, even if the payment is illegally applied for, the stop of the connection via the communication network cannot be cancelled from an external unit. Therefore, high security can be assured against the illegal payment application in association with the loss or theft of the card.

[0043] Although the above embodiment has been described with respect to the example in the case where the PHS telephone function is provided for the electronic money card, naturally, the PHS telephone function can be also replaced with an ordinary mobile phone function.

[0044] Although the payment has been applied for via the Internet in the foregoing embodiment, any communication network other than the Internet can be also used. According to a desirable embodiment of the invention, it is sufficient to use networks such that the network for payment application and the network for payment execution are different. It is sufficient to provide a time lag between the payment application and the payment execution. Therefore, the invention is not limited by the kind of network.

[0045] Although the above embodiment has been described with respect to the example in the case where a personal computer of the user is used as a terminal apparatus which is used for payment application, a PAD (PDA, mobile terminal etc.) or, for example, an ordinary mobile phone can be used so long as it is equipment having the Internet connecting function.

[0046] The above embodiment has been described with respect to the example in the case where money is withdrawn from the bank and deposited in the electronic money card. However, also with respect to a purchase application and a payment execution upon Internet online shopping in other cases, similarly, by making the purchase application from the terminal apparatus via the Internet and by setting the payment date/time or presetting it with a time lag, the payment by the electronic money card by electronic money or a credit is executed. Also in this case, similarly, since there is a time lag between

the purchase application and the payment execution, high security can be assured against the theft or loss of the electronic money card.

[0047] In addition, although in the above embodiment the electronic money card is connected to the terminal via a card slot, there is no need for any physical contact between the card and the terminal. The card may for example be retained in the user's wallet and coupled to the terminal by short-range wireless communication.

[0048] The invention is not limited to the foregoing embodiment but incorporates many proper modifications without losing the advantages of the invention. Further, the invention is not limited by the numerical values shown in the above embodiment.

[0049] As described above, the invention relates to an electronic money processing method for performing a card withdrawal of electronic money by an electronic money card having a simple mobile phone (Personal Handyphone System: PHS) function, a terminal apparatus of the user, and a bank server, a program for realizing such a method, and a recording medium. More particularly, the invention relates to an electronic money processing method which improves security by providing a time lag between application for payment by the Internet and execution of the payment by a mobile phone network, a program for realizing such a method, and a recording medium.

Claims

1. An electronic money processing method for a bank server which is connected to a terminal apparatus of the user via the Internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function, comprising:

   a payment accepting step wherein payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated is received from said terminal apparatus; and
   a payment executing step wherein when said payment date/time comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

2. A method according to claim 1, wherein in said payment accepting step, as said payment date/time, said terminal apparatus is notified of a selection screen of real-time payment and a designated payment date/time, thereby allowing the user to select either of them.

3. A method according to claim 1 or 2, wherein in said payment accepting step, the payment date/time which has been set in a manner such that as said payment money amount is larger, a time lag between said payment application date/time and a payment execution date/time is increased.

4. A method according to claim 1, 2, or 3, wherein in said payment accepting step, prior to accepting the payment, predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is received from said terminal apparatus and collated with a customer database, and when they coincide as a result of said collation, a next inputting process is authenticated.

5. A method according to claim 4, wherein said user authentication information includes a name, an address, and a personal identification number inputted by the user in addition to the account number and the telephone number obtained from said electronic money card.

6. A method according to any preceding claim, wherein in said payment executing step, if a telephone talk connection is not established in a telephone call to said electronic money card, the execution of the payment is stopped and the payment application is cancelled.

7. A method according to any preceding claim, wherein in said payment executing step, the execution of the payment is stopped by inputting a payment stop before said payment date/time, and the payment application is cancelled.

8. An electronic money processing method for a bank server which is connected to a terminal apparatus of the user via the Internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function, comprising:

   a payment accepting step wherein payment application in which a payment money amount has been designated is received from said terminal apparatus; and
   a payment executing step wherein a payment date/time is set by changing a time lag from a payment application date/time at which said payment application has been received in accordance with said accepted payment money amount, when said payment date/time comes, a telephone call is made to said electronic mon-

ey card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

9. A method according to claim 8, further comprising the step of notifying said terminal apparatus of said set payment date/time.

10. A method according to claim 8 or 9, wherein in said payment executing step, as said payment money amount is larger, a time lag between said payment application date/time and a payment execution date/time is increased.

11. A method according to claim 8, 9 or 10, wherein in said payment accepting step, prior to accepting the payment, predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is received from said terminal apparatus and collated with a customer database, and when they coincide as a result of said collation, a next inputting process is authenticated.

12. A method according to claim 11, wherein said user authentication information includes a name, an address, and a personal identification number inputted by the user in addition to the account number and the telephone number obtained from said electronic money card.

13. A method according to claim 8, 9, 10, 11, or 12, wherein in said payment executing step, if the telephone talk connection is not established in the telephone call to said electronic money card, the execution of the payment is stopped and the payment application is cancelled.

14. A method according to any of claims 8 to 13, wherein in said payment executing step, the execution of the payment is stopped by inputting a payment stop before said payment date/time, and the payment application is cancelled.

15. A program for processing electronic money, wherein

said program allows a computer constructing a bank server which is connected to a terminal apparatus of the user via the Internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function to execute:

a payment accepting step wherein payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated is received from said terminal apparatus; and
a payment executing step wherein when said payment date/time comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

16. A program for processing electronic money, wherein said program allows a computer constructing a bank server which is connected to a terminal apparatus of the user via the Internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function to execute:

a payment accepting step wherein payment application in which a payment money amount has been designated is received from said terminal apparatus; and
a payment executing step wherein a payment date/time is set by changing a time lag from a payment application date/time at which said payment application has been received in accordance with said accepted payment money amount, when said payment date/time comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

17. A computer-readable recording medium in which a program for processing electronic money has been stored, wherein

said program allows a computer constructing a bank server which is connected to a terminal apparatus of the user via the Internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function to execute:

a payment accepting step wherein payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated is received from said terminal apparatus; and
a payment executing step wherein when said payment date/time comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

18. A computer-readable recording medium in which a program for processing electronic money has been stored, wherein

said program allows a computer constructing a bank server which is connected to a terminal apparatus of the user via the internet and connected via a mobile phone network to an electronic money card having an interface that can be connected to said terminal apparatus and a mobile phone function to execute:

a payment accepting step wherein payment application in which a payment money amount has been designated is received from said terminal apparatus; and

a payment executing step wherein a payment date/time is set by changing a time lag from a payment application date/time at which said payment application has been received in accordance with said accepted payment money amount, when said payment date/time comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

19. An electronic money processing method for a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network, comprising:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to said bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated,

wherein when said payment date/time comes, a telephone call is made from said bank server to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

20. A method according to claim 19, wherein in said payment applying step, real-time payment and a designated payment date/time are prepared as said payment date/time, thereby allowing the user to select either of them.

21. A method according to claim 19 or 20, wherein in said payment applying step, as said payment money amount is larger, a time lag between said payment application date/time and said payment date/time is increased.

22. A method according to claim 19, 20, or 21, wherein in said authentication obtaining step, said user authentication information includes a name, an address, and a personal identification number inputted by the user in addition to the account number and the telephone number obtained from said electronic money card.

23. An electronic money processing method for a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network, comprising:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount has been designated,

wherein when a payment date/time which has been set by changing a time lag from a payment application date/time at which said payment application is received in accordance with said payment money amount accepted by said bank server comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

24. A program for processing electronic money, wherein

said program allows a computer constructing a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network to execute:

an authentication obtaining step wherein pre-

determined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to said bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated,

and wherein when said payment date/time comes, a telephone call is made from said bank server to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

25. A program for processing electronic money, wherein

said program allows a computer constructing a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount has been designated,

and wherein when a payment date/time which has been set by changing a time lag from a payment application date/time at which said payment application is received in accordance with said payment money amount accepted by said bank server comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

26. A computer-readable recording medium in which a program for processing electronic money has been stored, wherein

said program allows a computer constructing a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to said bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount and a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount have been designated,

and wherein when said payment date/time comes, a telephone call is made from said bank server to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

27. A computer-readable recording medium in which a program for processing electronic money has been stored, wherein

said program allows a computer constructing a terminal apparatus in which an electronic money card having an interface and a mobile phone function is connected to a card slot and which is connected via the internet to a bank server that is connected to said electronic money card via a mobile phone network to execute:

an authentication obtaining step wherein predetermined user authentication information including an account number and a telephone number obtained from said electronic money card is transmitted from said terminal apparatus to the bank server and authentication is obtained; and

a payment applying step wherein said bank server is notified of payment application in which a payment money amount has been designated,

and wherein when a payment date/time which has been set by changing a time lag from a payment application date/time at which said payment application is received in accordance with said payment money amount accepted by said bank server comes, a telephone call is made to said electronic money card, establishment of a telephone talk connection is confirmed, and payment of the electronic money is executed.

28. A processing method for an electronic money card which is connected to a terminal apparatus of the user via a card slot and connected to a bank server via a mobile phone network, comprising:

a payment supporting step wherein when payment application in which at least a payment money amount has been designated is notified to said bank server by said terminal apparatus, his own telephone number and account number which have previously been stored are provided; and

a payment receiving step wherein when a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount comes, if a telephone call is received from said bank server, establishment of a telephone talk connection is confirmed, and payment of the electronic money is received.

29. A method according to claim 28, wherein in said payment receiving step, it is discriminated that a phone number of an originator obtained by a telephone call from said bank server lies within a predetermined bank telephone number range which has previously been stored, and an automatic response is made, thereby establishing the telephone talk connection.

30. A program for processing electronic money, wherein

said program allows a computer of an electronic money card which is connected to a terminal apparatus of the user via a card slot and connected to a bank server via a mobile phone network to execute:

a payment supporting step wherein when payment application in which at least a payment money amount has been designated is notified to said bank server by said terminal apparatus, his own telephone number and account number which have previously been stored are provided; and

a payment receiving step wherein when a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount comes, if a telephone call is received from said bank server, establishment of a telephone talk connection is confirmed, and payment of the electronic money is received.

31. A computer-readable recording medium in which a program for processing electronic money has been stored, wherein

said program allows a computer of an electronic money card which is connected to a terminal apparatus of the user via a card slot and connected to a bank server via a mobile phone network to execute:

a payment supporting step wherein when payment application in which at least a payment money amount has been designated is notified to said bank server by said terminal apparatus, his own telephone number and account number which have previously been stored are provided; and

a payment receiving step wherein when a payment date/time which has been set by changing a time lag from a payment application date/time in accordance with said payment money amount comes, if a telephone call is received from said bank server, establishment of a telephone talk connection is confirmed, and payment of the electronic money is received.

FIG. 1

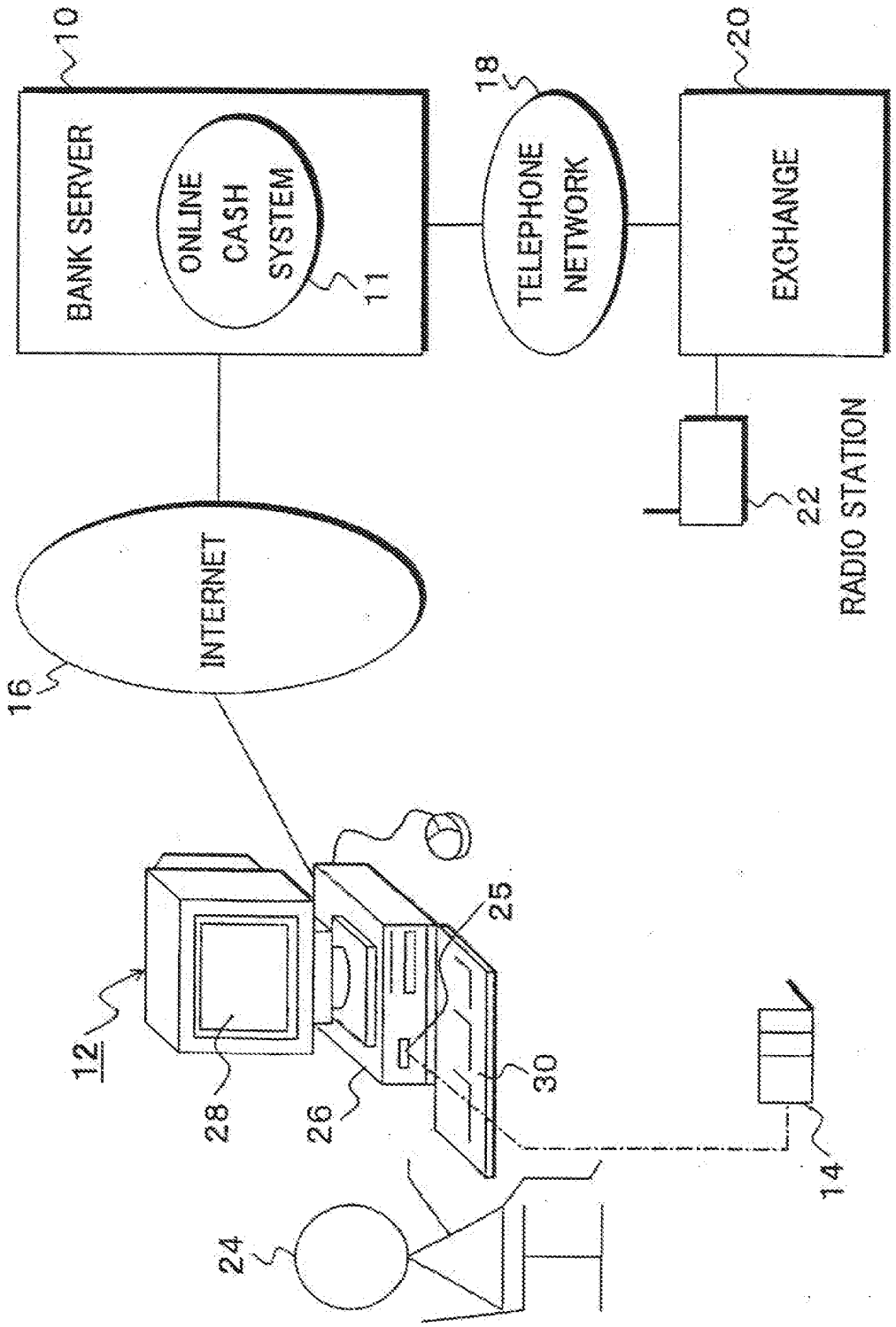

10
BANK SERVER
ONLINE CASH SYSTEM
11
18
TELEPHONE NETWORK
20
EXCHANGE
22
RADIO STATION
16
INTERNET
12
25
28
26
30
14
24

FIG. 2

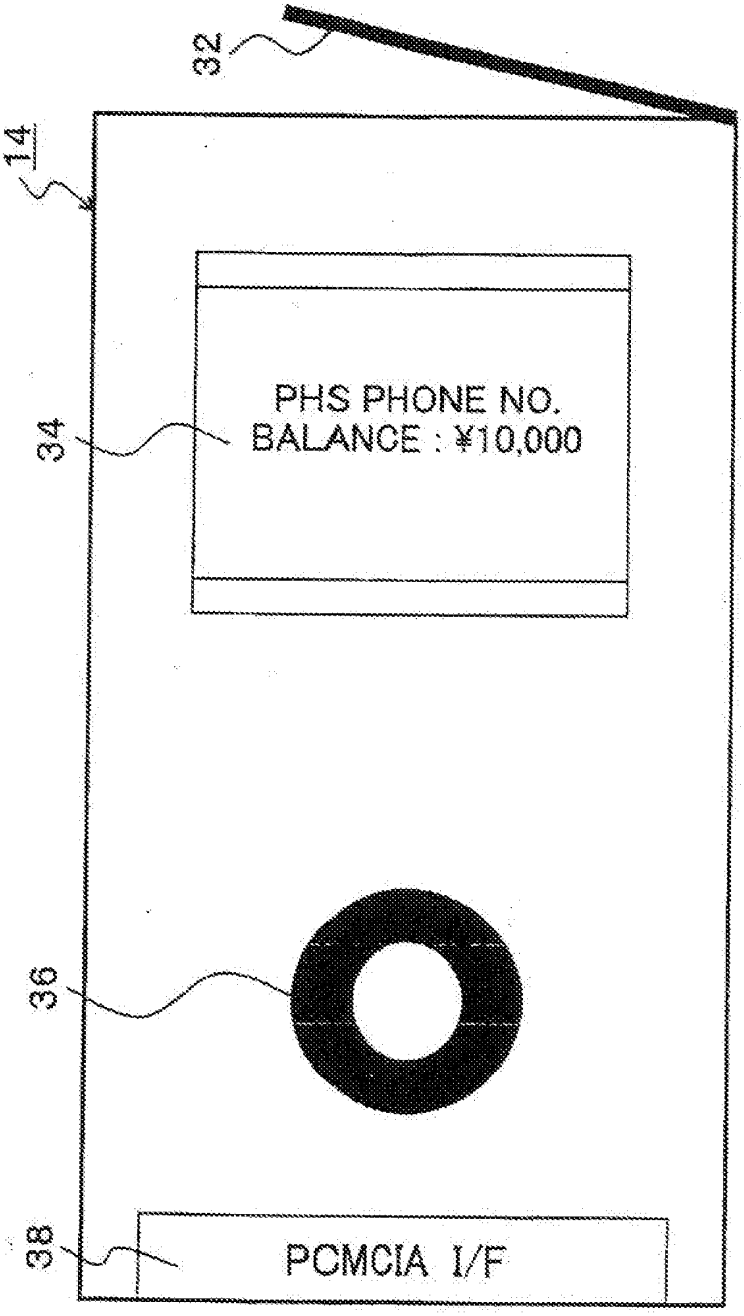


FIG. 3

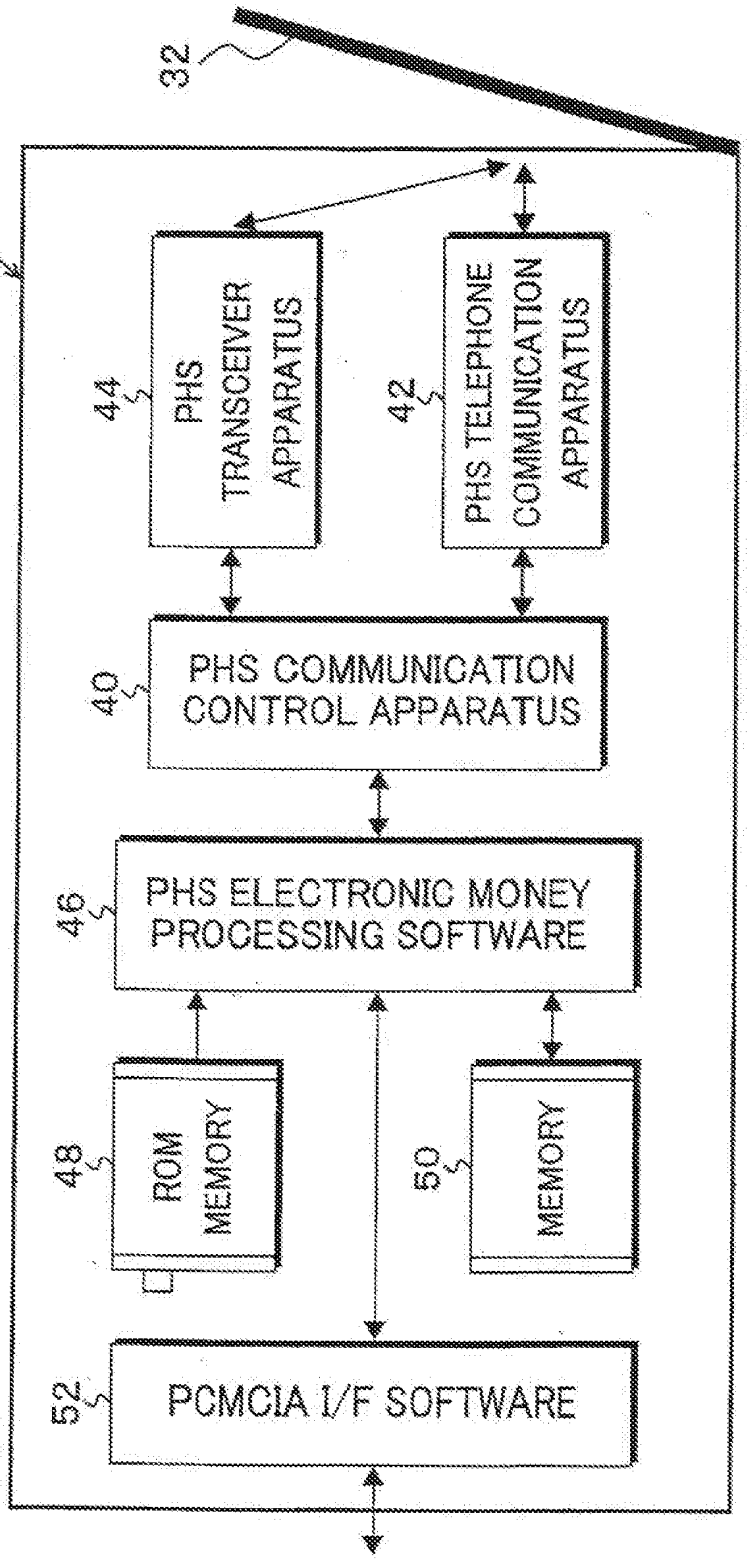

32
14
44
PHS TRANSCEIVER APPARATUS
42
PHS TELEPHONE COMMUNICATION APPARATUS
40
PHS COMMUNICATION CONTROL APPARATUS
46
PHS ELECTRONIC MONEY PROCESSING SOFTWARE
48
ROM MEMORY
50
MEMORY
52
PCMCIA I/F SOFTWARE

FIG. 4

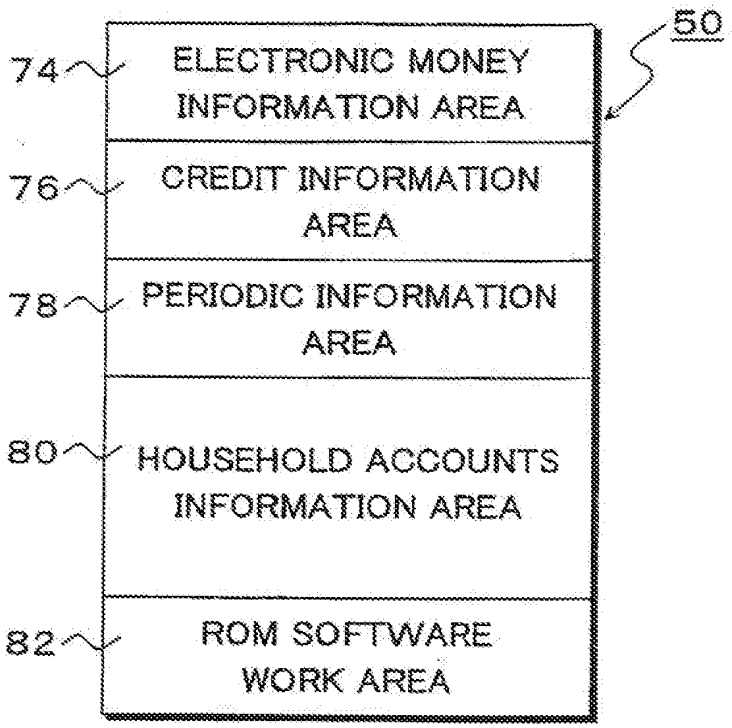

50
74
ELECTRONIC MONEY INFORMATION AREA
76
CREDIT INFORMATION AREA
78
PERIODIC INFORMATION AREA
80
HOUSEHOLD ACCOUNTS INFORMATION AREA
82
ROM SOFTWARE WORK AREA

FIG. 5A

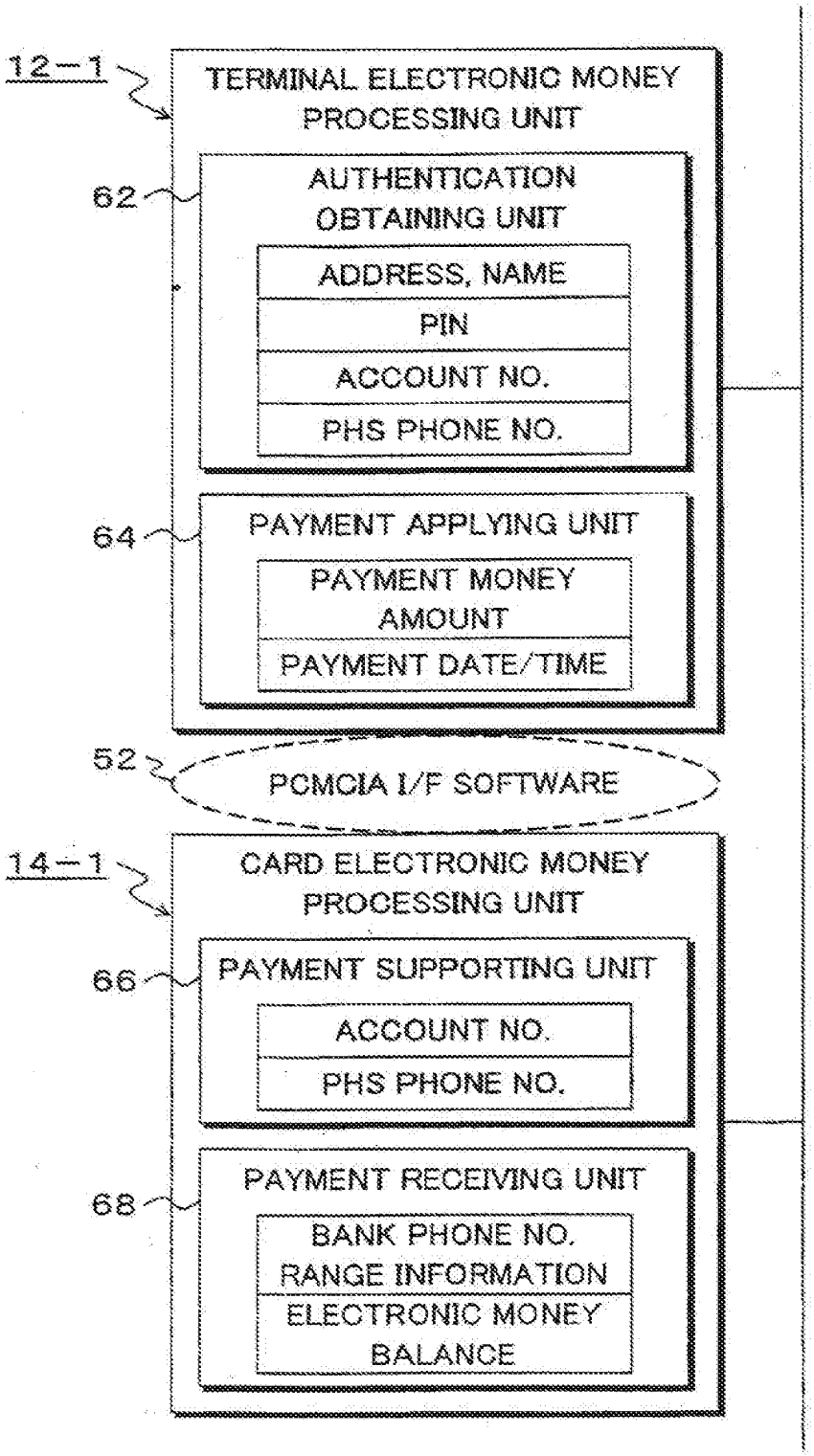

12-1
TERMINAL ELECTRONIC MONEY PROCESSING UNIT
62
AUTHENTICATION OBTAINING UNIT
ADDRESS, NAME
PIN
ACCOUNT NO.
PHS PHONE NO.
64
PAYMENT APPLYING UNIT
PAYMENT MONEY AMOUNT
PAYMENT DATE/TIME
52
PCMCIA I/F SOFTWARE
14-1
CARD ELECTRONIC MONEY PROCESSING UNIT
66
PAYMENT SUPPORTING UNIT
ACCOUNT NO.
PHS PHONE NO.
68
PAYMENT RECEIVING UNIT
BANK PHONE NO. RANGE INFORMATION
ELECTRONIC MONEY BALANCE

FIG. 5B

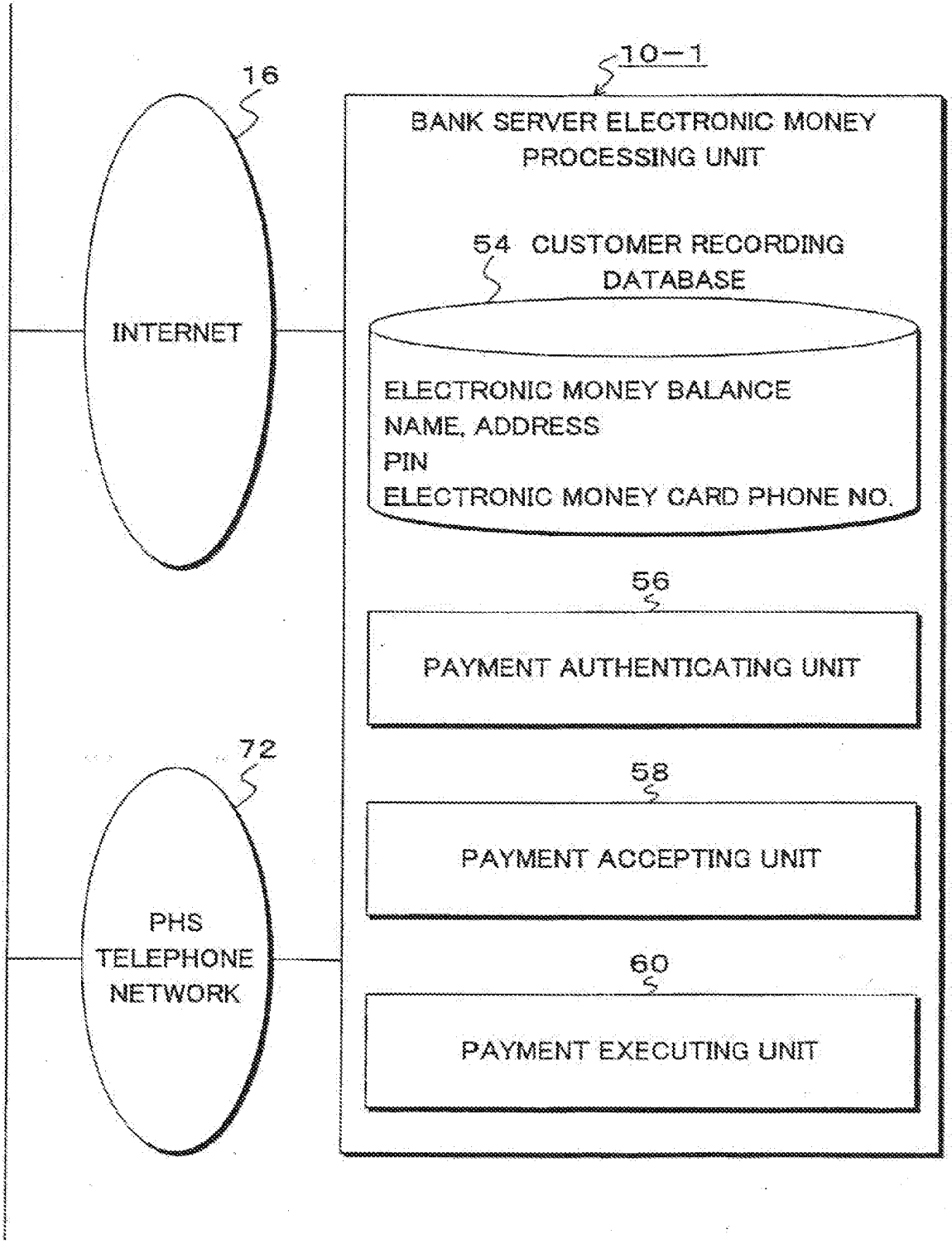

10-1
16
BANK SERVER ELECTRONIC MONEY PROCESSING UNIT
54 CUSTOMER RECORDING DATABASE
INTERNET
ELECTRONIC MONEY BALANCE
NAME, ADDRESS
PIN
ELECTRONIC MONEY CARD PHONE NO.
56
PAYMENT AUTHENTICATING UNIT
72
58
PAYMENT ACCEPTING UNIT
PHS TELEPHONE NETWORK
60
PAYMENT EXECUTING UNIT

FIG. 6A

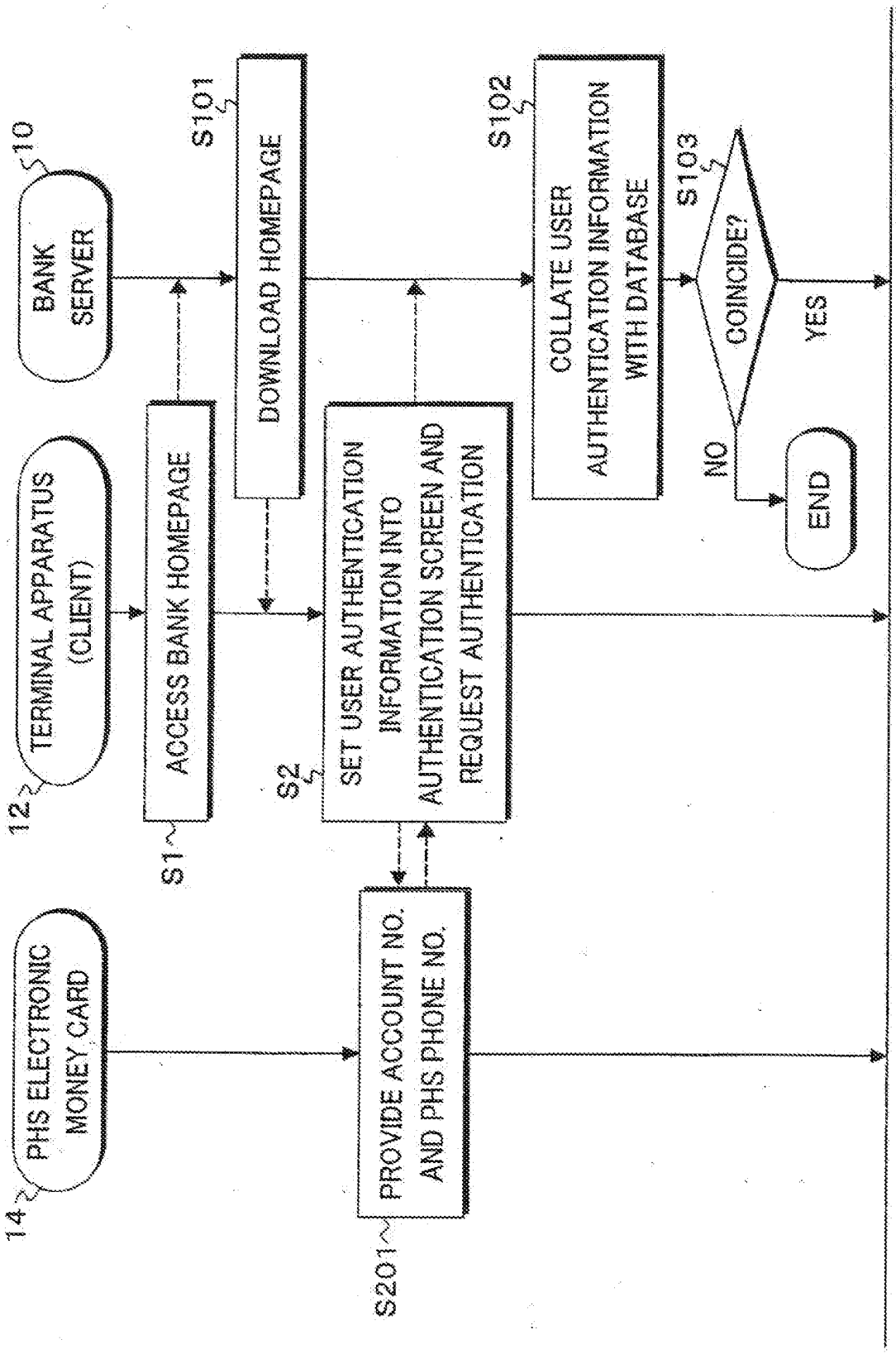

BANK SERVER
10
TERMINAL APPARATUS (CLIENT)
12
PHS ELECTRONIC MONEY CARD
14
ACCESS BANK HOMEPAGE
S1
DOWNLOAD HOMEPAGE
S101
SET USER AUTHENTICATION INFORMATION INTO AUTHENTICATION SCREEN AND REQUEST AUTHENTICATION
S2
PROVIDE ACCOUNT NO. AND PHS PHONE NO.
S201
COLLATE USER AUTHENTICATION INFORMATION WITH DATABASE
S102
COINCIDE?
S103
NO
YES
END

FIG. 6B

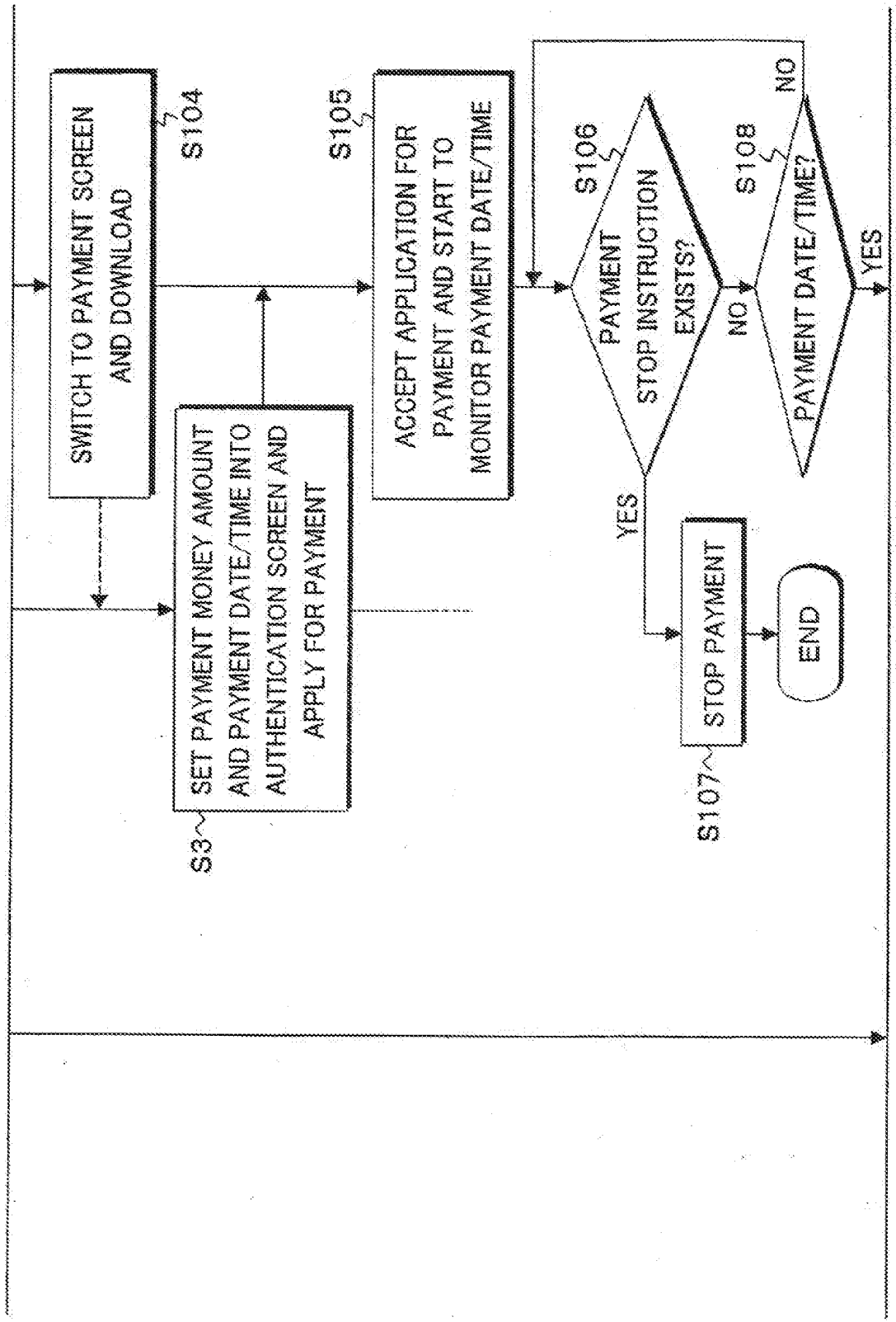

SWITCH TO PAYMENT SCREEN AND DOWNLOAD
S104
S105
ACCEPT APPLICATION FOR PAYMENT AND START TO MONITOR PAYMENT DATE/TIME
S3
SET PAYMENT MONEY AMOUNT AND PAYMENT DATE/TIME INTO AUTHENTICATION SCREEN AND APPLY FOR PAYMENT
S106
PAYMENT STOP INSTRUCTION EXISTS?
YES
NO
S108
PAYMENT DATE/TIME?
NO
YES
S107
STOP PAYMENT
END

FIG. 6C

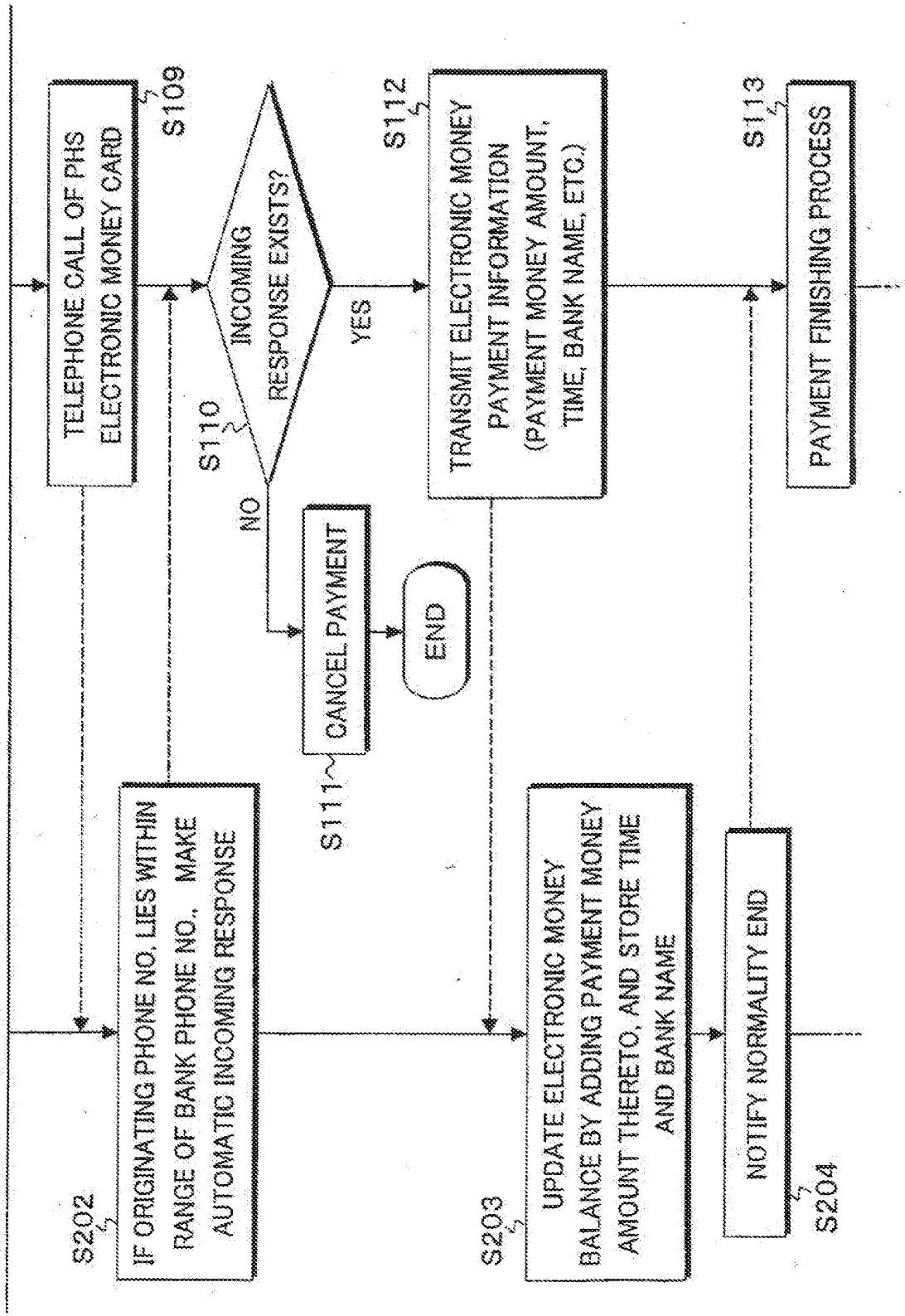

TELEPHONE CALL OF PHS ELECTRONIC MONEY CARD
S109
INCOMING RESPONSE EXISTS?
S110
NO
YES
CANCEL PAYMENT
S111
END
S112
TRANSMIT ELECTRONIC MONEY PAYMENT INFORMATION (PAYMENT MONEY AMOUNT, TIME, BANK NAME, ETC.)
S113
PAYMENT FINISHING PROCESS
S202
IF ORIGINATING PHONE NO. LIES WITHIN RANGE OF BANK PHONE NO., MAKE AUTOMATIC INCOMING RESPONSE
S203
UPDATE ELECTRONIC MONEY BALANCE BY ADDING PAYMENT MONEY AMOUNT THERETO, AND STORE TIME AND BANK NAME
NOTIFY NORMALITY END
S204

FIG. 7A

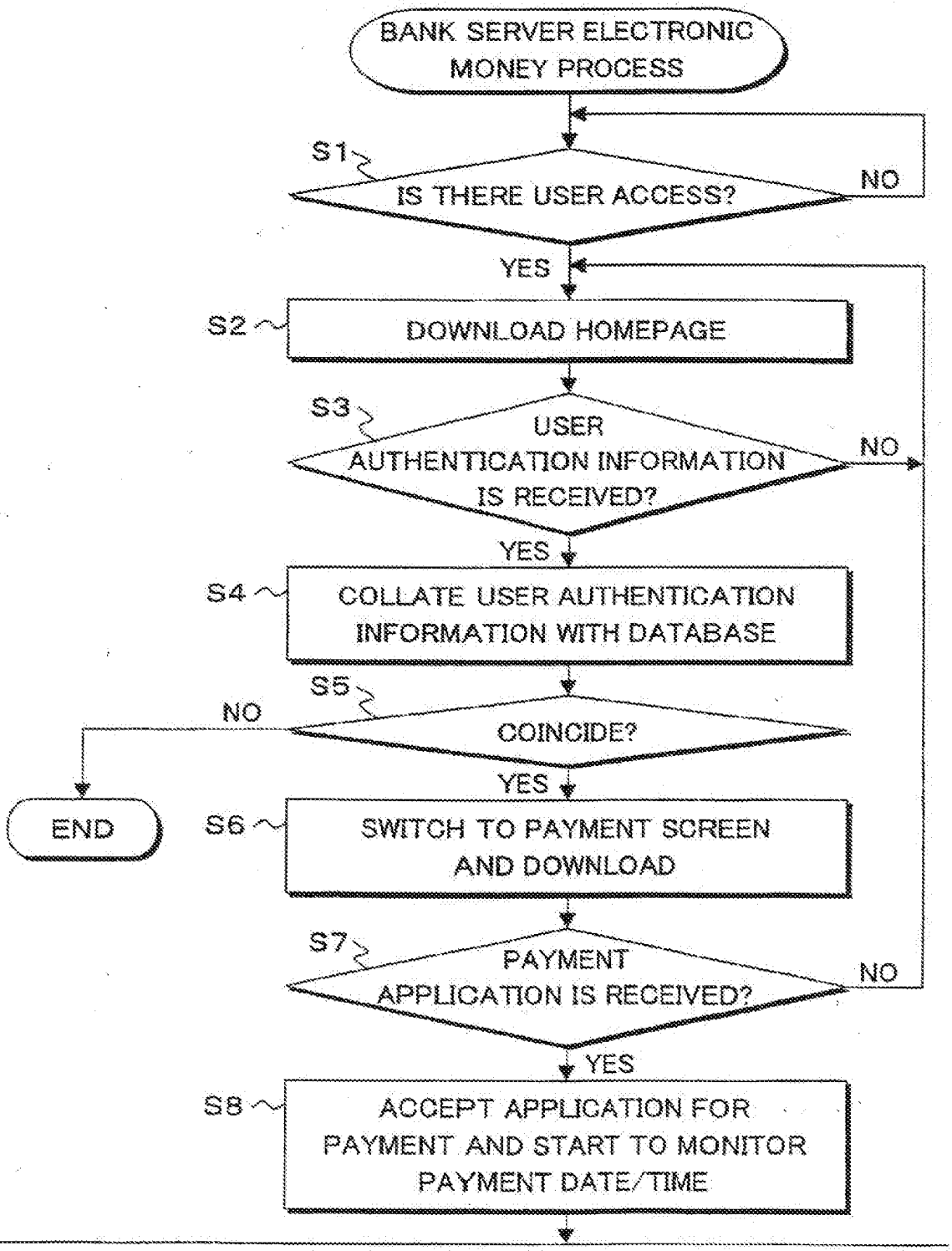

BANK SERVER ELECTRONIC MONEY PROCESS
S1
IS THERE USER ACCESS?
NO
YES
S2
DOWNLOAD HOMEPAGE
S3
USER AUTHENTICATION INFORMATION IS RECEIVED?
NO
YES
S4
COLLATE USER AUTHENTICATION INFORMATION WITH DATABASE
S5
COINCIDE?
NO
YES
END
S6
SWITCH TO PAYMENT SCREEN AND DOWNLOAD
S7
PAYMENT APPLICATION IS RECEIVED?
NO
YES
S8
ACCEPT APPLICATION FOR PAYMENT AND START TO MONITOR PAYMENT DATE/TIME

FIG. 7B

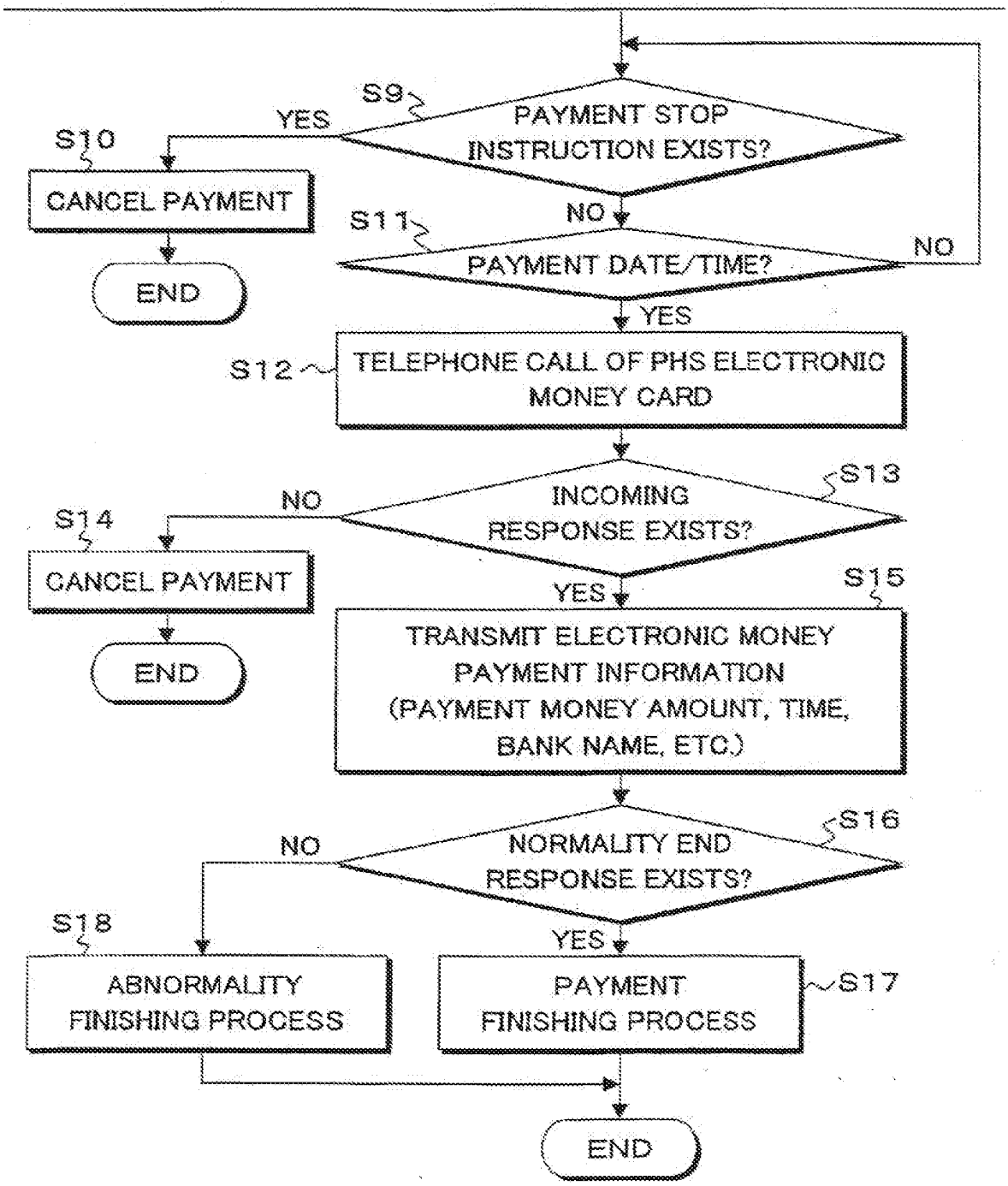

S9
PAYMENT STOP INSTRUCTION EXISTS?
YES
S10
CANCEL PAYMENT
END
NO
S11
PAYMENT DATE/TIME?
NO
YES
S12
TELEPHONE CALL OF PHS ELECTRONIC MONEY CARD
S13
INCOMING RESPONSE EXISTS?
NO
S14
CANCEL PAYMENT
END
YES
S15
TRANSMIT ELECTRONIC MONEY PAYMENT INFORMATION (PAYMENT MONEY AMOUNT, TIME, BANK NAME, ETC.)
S16
NORMALITY END RESPONSE EXISTS?
NO
S18
ABNORMALITY FINISHING PROCESS
YES
PAYMENT FINISHING PROCESS
S17
END

FIG. 8A

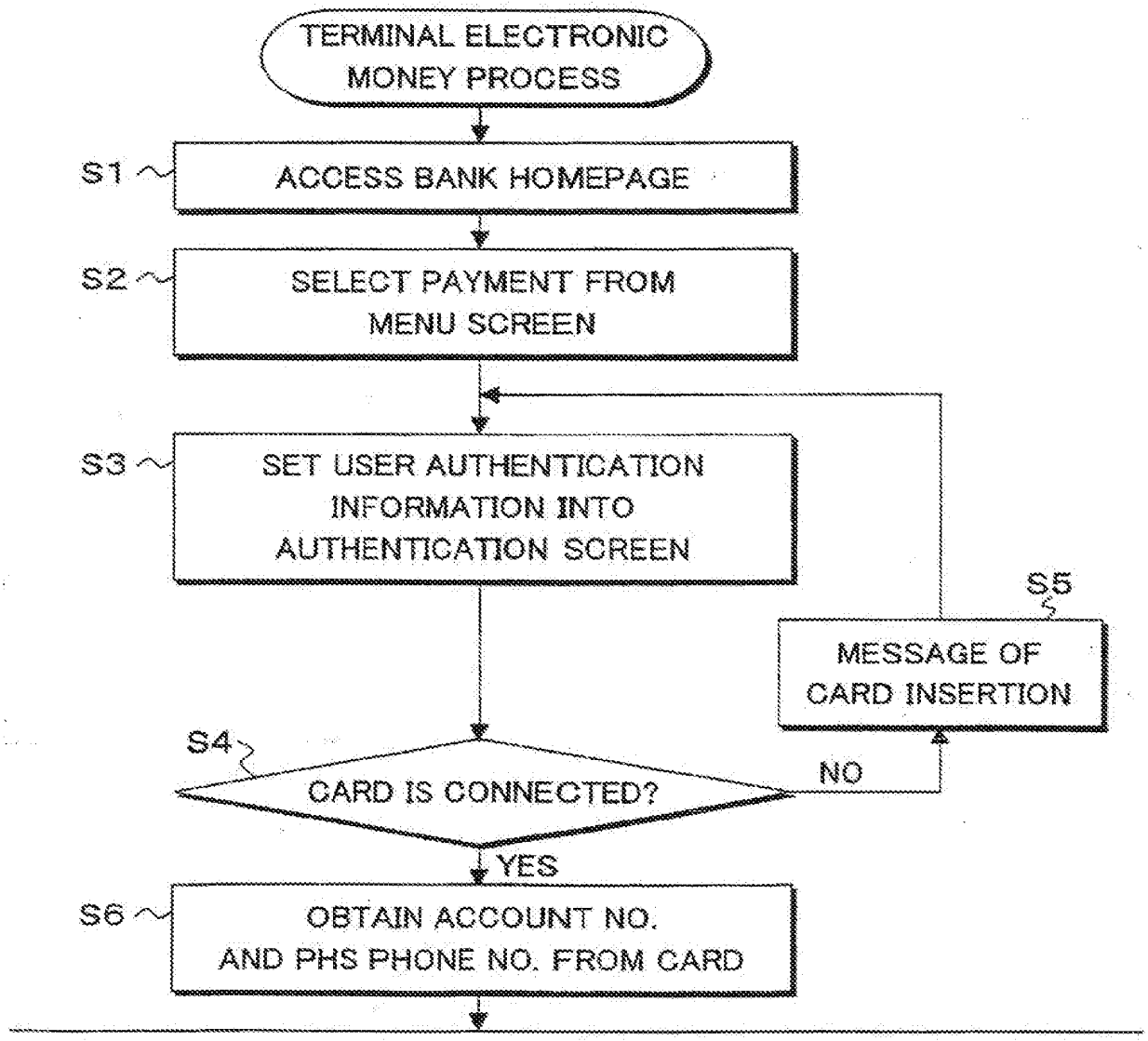

TERMINAL ELECTRONIC MONEY PROCESS
S1
ACCESS BANK HOMEPAGE
S2
SELECT PAYMENT FROM MENU SCREEN
S3
SET USER AUTHENTICATION INFORMATION INTO AUTHENTICATION SCREEN
S5
MESSAGE OF CARD INSERTION
S4
CARD IS CONNECTED?
NO
YES
S6
OBTAIN ACCOUNT NO. AND PHS PHONE NO. FROM CARD

FIG. 8B

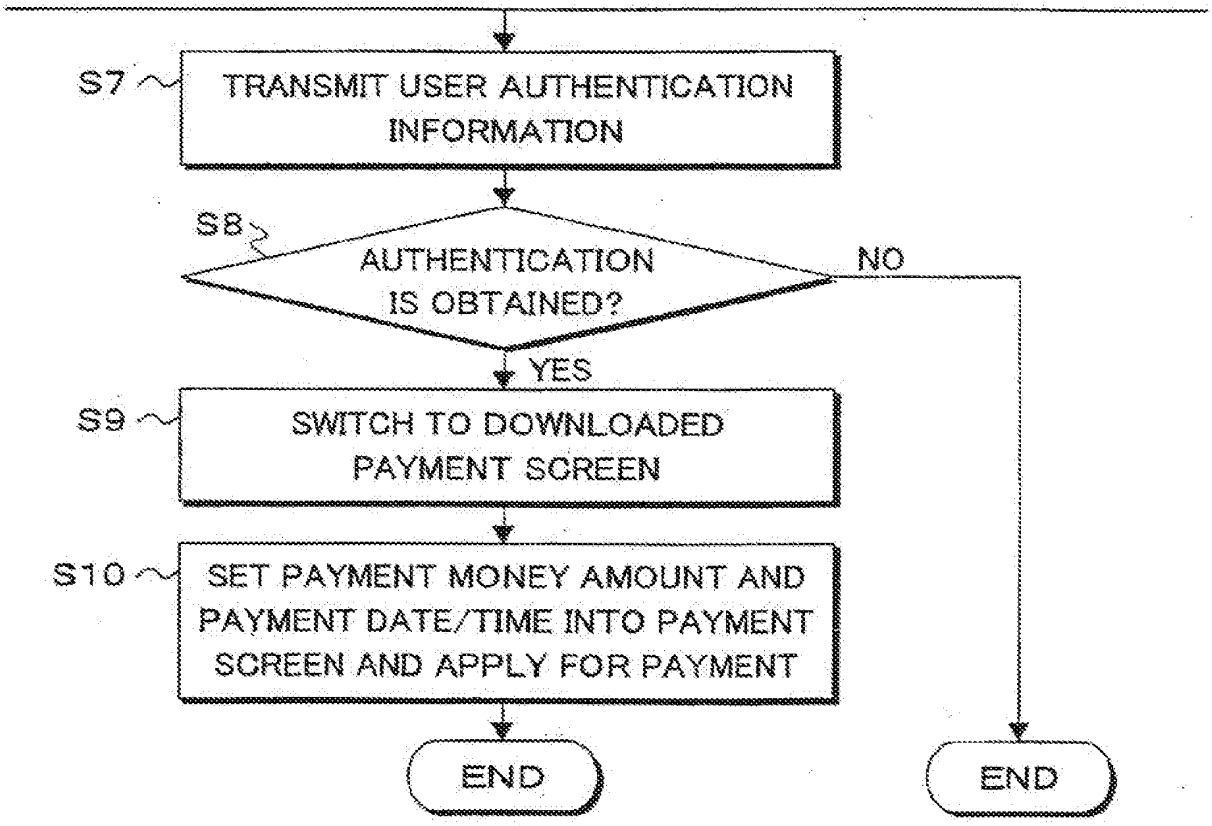

S7
TRANSMIT USER AUTHENTICATION INFORMATION
S8
AUTHENTICATION IS OBTAINED?
NO
YES
S9
SWITCH TO DOWNLOADED PAYMENT SCREEN
S10
SET PAYMENT MONEY AMOUNT AND PAYMENT DATE/TIME INTO PAYMENT SCREEN AND APPLY FOR PAYMENT
END
END

FIG. 9A

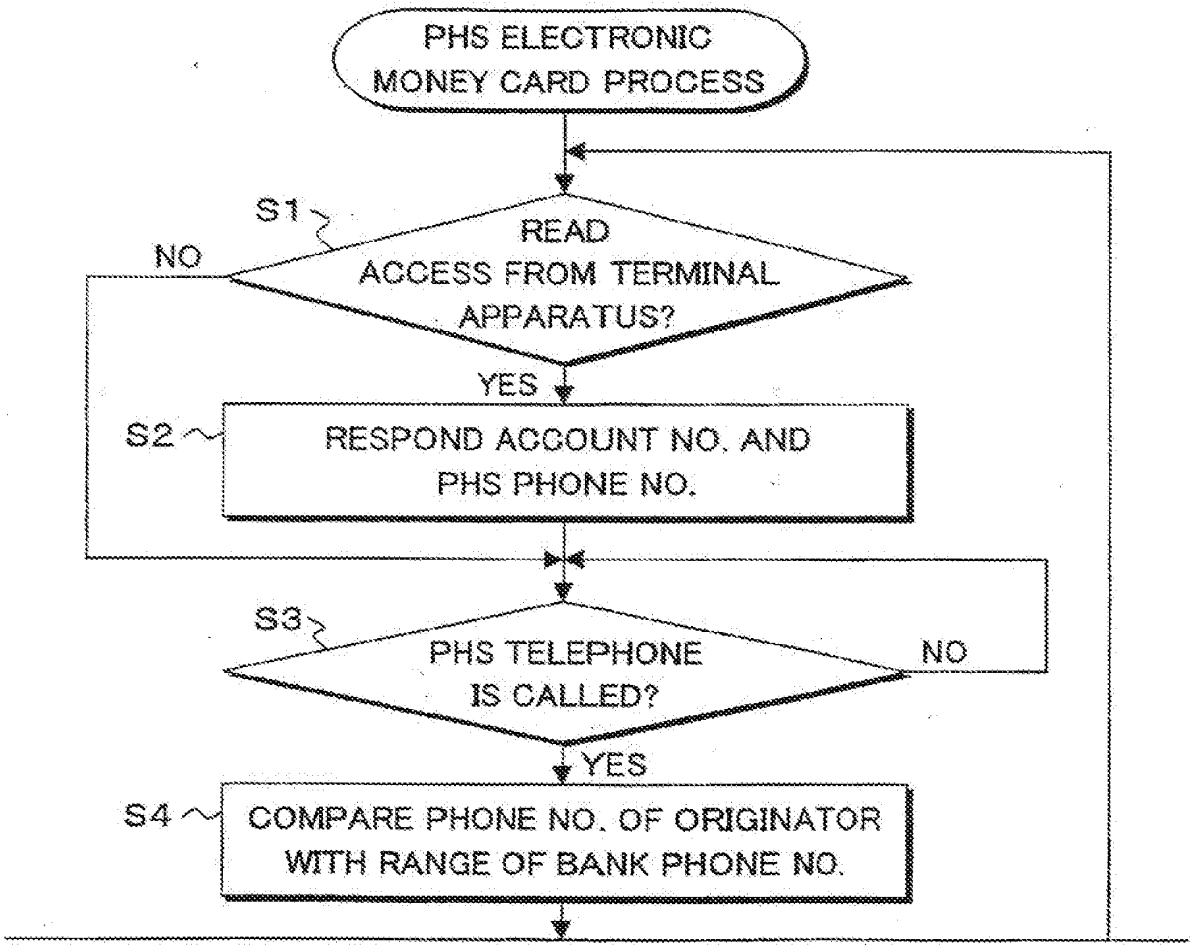
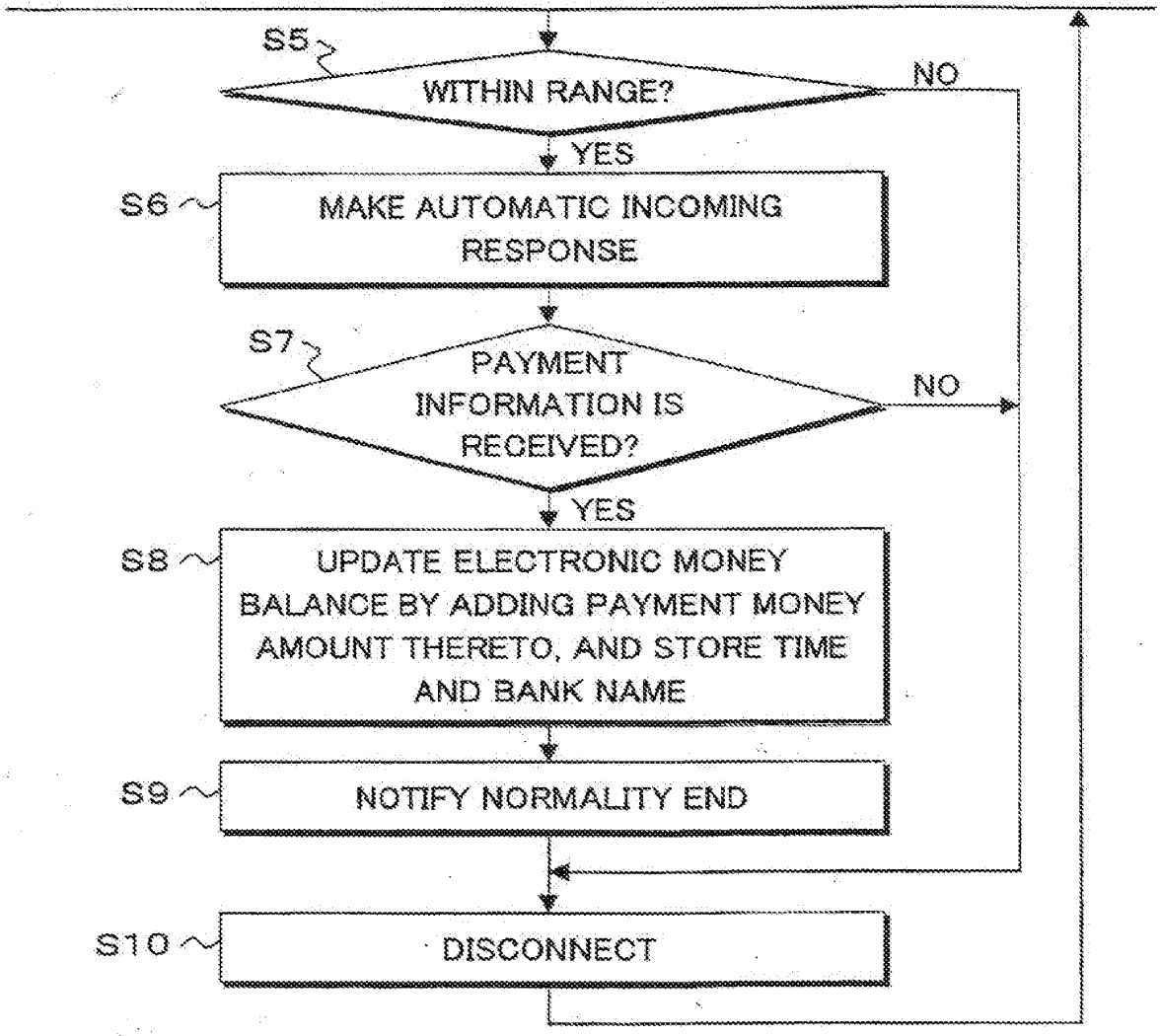

PHS ELECTRONIC MONEY CARD PROCESS
S1
READ ACCESS FROM TERMINAL APPARATUS?
NO
YES
S2
RESPOND ACCOUNT NO. AND PHS PHONE NO.
S3
PHS TELEPHONE IS CALLED?
NO
YES
S4
COMPARE PHONE NO. OF ORIGINATOR WITH RANGE OF BANK PHONE NO.

FIG. 9B


S5
WITHIN RANGE?
NO
YES
S6
MAKE AUTOMATIC INCOMING RESPONSE
S7
PAYMENT INFORMATION IS RECEIVED?
NO
YES
S8
UPDATE ELECTRONIC MONEY BALANCE BY ADDING PAYMENT MONEY AMOUNT THERETO, AND STORE TIME AND BANK NAME
S9
NOTIFY NORMALITY END
S10
DISCONNECT

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 075 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
13.07.2005 Bulletin 2005/28

(51) Int Cl.7: **G07F 19/00**

(43) Date of publication A2:
21.05.2003 Bulletin 2003/21

(21) Application number: **02251152.1**

(22) Date of filing: **20.02.2002**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 JP 2001352947**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

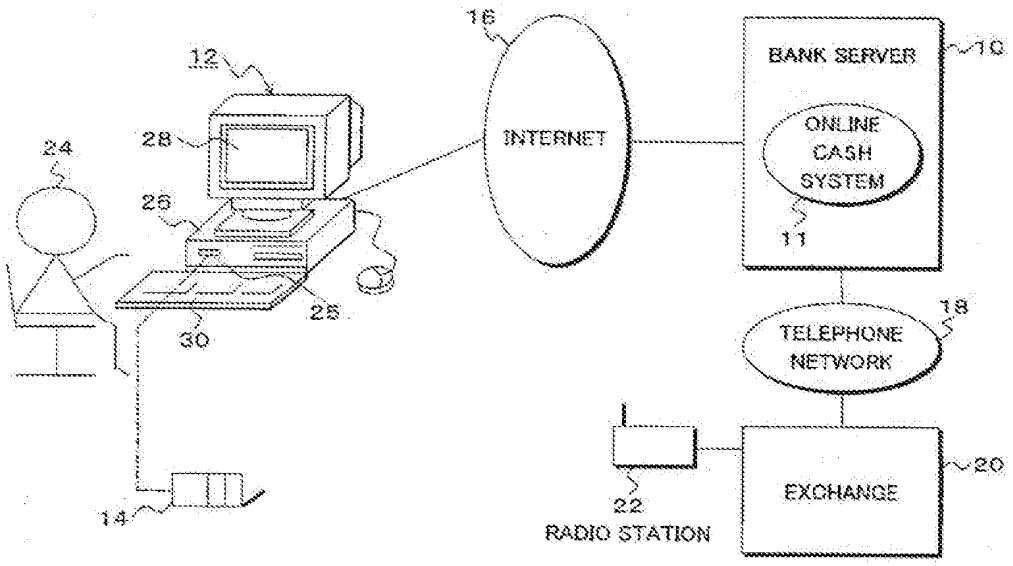
(72) Inventor: **Okamura, Michio, c/o Fujitsu Limited**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative: **Stebbing, Timothy Charles et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Electronic money processing method and program

(57) An electronic money system is constructed by: a terminal apparatus (12) of the user; an electronic money card (14) having an interface which can be connected to the terminal apparatus and a mobile phone function; and a bank server (10) which is connected to the terminal apparatus via the internet (16) and connected to the electronic money card (14) via a mobile telephone network. A payment request in which a payment money amount and a payment date/time have been designated is notified to the bank server (10) by the terminal apparatus (12). When the payment date/time arrives, a telephone call is made from the bank server to the electronic money card, establishment of a connection is confirmed, and payment of electronic money to the card is executed. By setting a payment date/time in the future, payment to a lost or stolen card can be prevented.

FIG. 1



EP 1 313 075 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 1152

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	DE 197 24 901 A1 (SIEMENS NIXDORF INFORMATIONSSYSTEME AG, 33106 PADERBORN, DE) 17 December 1998 (1998-12-17) * abstract; claims; figure 1 * * column 1, line 3 - line 6 * * column 1, line 27 - line 30 * * column 1, line 39 - line 61 * * column 2, line 17 - line 26 * * column 2, line 37 - line 62 * * column 3, line 17 - line 32 * * column 3, line 37 - line 53 * * column 4, line 41 - line 53 *	1-33	G07F19/00
A	DE 199 36 226 A1 (ALCATEL, PARIS) 8 February 2001 (2001-02-08) * abstract; claims 1,2,9-11,13,14; figure 1 * * column 2, line 11 - line 61 * * column 3, line 46 - column 4, line 60 *	1-33	
A	US 6 064 990 A (GOLDSMITH ET AL) 16 May 2000 (2000-05-16) * abstract; claim 1; figures 1,2 * * column 1, line 51 - line 64 *	1-33	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07F H04L G06F
A	WO 98/54943 A (HO KEUNG, TSE; TSE, HO KEUNG) 10 December 1998 (1998-12-10) * abstract * * page 4 - page 7; figure 2 *	1-33	
A	WO 95/19593 A (KEW, MICHAEL, JEREMY; LOVE, JAMES, SIMON) 20 July 1995 (1995-07-20) * the whole document *		
A	WO 01/82162 A (COMPUTER APPLICATIONS CO., LTD; UEHARA, TSUYOSHI; MURAKAMI, MASAHARU) 1 November 2001 (2001-11-01) * abstract *		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	25 May 2005	Rother, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 25 1152

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-05-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19724901 A1	17-12-1998	CA 2293554 A1	17-12-1998
		WO 9857510 A2	17-12-1998
		EP 1002437 A2	24-05-2000
DE 19936226 A1	08-02-2001	AT 263470 T	15-04-2004
		DE 50005859 D1	06-05-2004
		EP 1075161 A2	07-02-2001
US 6064990 A	16-05-2000	NONE	
WO 9854943 A	10-12-1998	AU 8019698 A	21-12-1998
		WO 9854943 A2	10-12-1998
		EP 1147497 A2	24-10-2001
WO 9519593 A	20-07-1995	AU 1390395 A	01-08-1995
		WO 9519593 A1	20-07-1995
		GB 2300288 A	30-10-1996
WO 0182162 A	01-11-2001	AU 7206801 A	07-11-2001
		CN 1439141 A	27-08-2003
		CN 1501308 A	02-06-2004
		CN 1510623 A	07-07-2004
		EP 1291794 A1	12-03-2003
		WO 0182162 A1	01-11-2001
		JP 3632919 B2	30-03-2005
		JP 2003178244 A	27-06-2003
		JP 2004038991 A	05-02-2004
		US 2004215572 A1	28-10-2004
		US 2004098307 A1	20-05-2004
		US 2004098338 A1	20-05-2004